技术商务资信评分明细 （专家1）

项目名称: 义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3.6	2.4	2.8	2
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4.5	3	3.5	2.5
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.6	2.4	2.8	2
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.9	0	0.5	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.9	0	0.5	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.9	0	0.5	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.9	0	0.5	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.9	0	0.4	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.9	0	0.4	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.9	0	0.7	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.9	0	0.7	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.9	0	0.5	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.9	0	0.5	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	1	0	0.3	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	1	0	0.3	0
合计			0-90	85.5	30	39.3	25.5

专家（签名）：

技术商务资信评分明细（专家2）

项目名称：义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	1.7	1.1	1.4	1
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3.5	2.5	3	2.2
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	2.6	2	2.2	1.9
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4.5	3.5	4	3.2
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	1.7	1.2	1.5	1.1

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.5	2.6	3	2.3
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	0.8	0.5	0.6	0.4
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	0.8	0.5	0.7	0.4
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.5	1.9	2.1	1.8
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.9	0	0.5	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.9	0	0.5	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.9	0	0.5	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.9	0	0.5	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.9	0	0.4	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.9	0	0.4	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.9	0	0.7	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.9	0	0.7	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.9	0	0.5	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.9	0	0.5	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	1	0	0.3	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	1	0	0.3	0
合计			0-90	84.6	30.8	40.3	27.3

专家（签名）：

技术商务资信评分明细（专家3）

项目名称：义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	1.5	1.2	1.5	1
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3.3	2.7	3	2.2
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	2.5	2.2	2.2	1.9
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4.5	3.8	4	3.3
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	1.6	1.3	1.5	1.2

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.5	2.7	3	2.3
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	0.8	0.5	0.6	0.4
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	0.8	0.5	0.7	0.4
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.3	2	2.2	1.8
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.8	0.3	0.5	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.8	0	0.5	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.8	0	0.5	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.8	0	0.5	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.8	0	0.5	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.8	0	0.5	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.8	0	0.7	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.8	0	0.7	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.8	0	0.6	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.8	0	0.6	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	0.9	0	0.4	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	0.9	0	0.3	0
合计			0-90	82.6	32.2	41	27.5

专家（签名）：

技术商务资信评分明细 （专家4）

项目名称: 义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3.6	2.4	2.8	2
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4.5	3	3.5	2.5
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.6	2.4	2.8	2
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.9	0	0.5	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.9	0	0.5	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.9	0	0.5	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.9	0	0.5	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.9	0	0.4	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.9	0	0.4	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.9	0	0.7	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.9	0	0.7	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.9	0	0.5	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.9	0	0.5	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	1	0	0.3	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	1	0	0.3	0
合计			0-90	85.5	30	39.3	25.5

专家（签名）：

技术商务资信评分明细（专家5）

项目名称：义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	2	1	1.5	0.5
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3	1.5	2	1
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	3	1.5	2	1
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4	2	3	1.5
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	2	1	1.5	0.5

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.5	2	3	1
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	1	1	1	1
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	1	1	1	1
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.5	1.5	2	2
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.8	0	0.9	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.8	0	0.9	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.8	0	0.8	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.8	0	0.9	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.8	0	0.8	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.8	0	0.9	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.8	0	0.9	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.9	0	0.9	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.8	0	0.9	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.8	0	0.9	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	0.8	0	0.9	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	0.8	0	0.8	0
合计			0-90	83.7	27.5	43.5	22.5

专家（签名）：

技术商务资信评分明细（专家6）

项目名称：义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3.6	2.4	2.8	2
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4.5	3	3.5	2.5
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.6	2.4	2.8	2
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.9	0	0.5	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.9	0	0.5	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.9	0	0.5	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.9	0	0.5	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.9	0	0.4	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.9	0	0.4	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.9	0	0.7	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.9	0	0.7	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.9	0	0.5	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.9	0	0.5	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	1	0	0.3	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	1	0	0.3	0
合计			0-90	85.5	30	39.3	25.5

专家（签名）：

技术商务资信评分明细（专家7）

项目名称：义乌市数据管理中心网络安全全链路监管服务项目（YWCG2022039GK）

序号	评分类型	评分项目内容	分值范围	联通（浙江）产业互联网有限公司	浙江众祺科技股份有限公司	中国电信股份有限公司义乌分公司	浙江索控科技有限公司
1	技术	同类业绩： 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。 投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。	0-1	1	0	0	0
2	技术	投标人能力体现： (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。	0-4	4	0	0	0
3.1	技术	投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1
3.2	技术	根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。	0-4	3.6	2.4	2.8	2
3.3	技术	根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
3.4	技术	根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。	0-5	4.5	3	3.5	2.5
4.1	技术	项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	5	0	0	0
4.2	技术	技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。	0-5	4	0	1	0
5.1	技术	根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。	0-2	1.8	1.2	1.4	1

5.2	技术	根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。	0-4	3.6	2.4	2.8	2
6.1	技术	根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.2	技术	根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。	0-1	0.9	0.6	0.7	0.5
6.3	技术	根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。	0-3	2.7	1.8	2.1	1.5
7	技术	服务能力指标： 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。	0-30	30	15	9	13
8.1.1	技术	（1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。	0-1	1	0	1	0
8.1.2	技术	（2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。	0-1	1	0	1	0
8.1.3	技术	（3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。	0-1	1	0	0	0
8.1.4	技术	（4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。	0-1	1	0	1	0
8.2.1	技术	（1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。	0-1	1	0	1	0
8.2.2	技术	（2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。	0-1	1	0	0	0
8.2.3	技术	（3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。	0-1	1	0	1	0
8.3.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。	0-1	0.9	0	0.5	0

8.3.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。	0-1	0.9	0	0.5	0
8.4.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。	0-1	0.9	0	0.5	0
8.4.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。	0-1	0.9	0	0.5	0
8.5.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。	0-1	0.9	0	0.4	0
8.5.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。	0-1	0.9	0	0.4	0
8.6.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。	0-1	0.9	0	0.7	0
8.6.2	技术	（2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。	0-1	0.9	0	0.7	0
8.7.1	技术	（1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。	0-1	0.9	0	0.5	0
8.7.2	技术	（2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。	0-1	0.9	0	0.5	0
8.8.1	技术	（1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。	0-1	1	0	1	0
8.9.1	技术	（1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等；	0-1	1	0	0.3	0
8.9.2	技术	（2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。	0-1	1	0	0.3	0
合计			0-90	85.5	30	39.3	25.5

专家（签名）：