

常州市公安局 2023 年度安全设备维保项目合同

项目名称：常州市公安局 2023 年度安全设备维保项目

甲方：常州市公安局

签订地点：常州市锦绣路 2 号 1-1

号

乙方：江苏移动信息系统集成有限公司 签订时间：2023 年 7 月 日

集中采购机构：常州市政府采购中心

根据常州市政府采购中心 2023 年 5 月 26 日进行的常采竞磋 [2023]0044 号招标，甲、乙双方就乙方中标的常州市公安局 2023 年度安全设备维保项目，本着平等互利的原则，通过共同协商，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及有关法律法规，就相关事宜达成如下合同。

一、总则

乙方按甲方要求，为甲方提供的常州市公安局 2023 年度安全设备维保项目具体服务内容见下表：

1、硬件设备

注：前 50 项，北京迅安、天行网安设备要求原厂维保。

序号	设备类型	型号	序列号	过保时间	维保期限(月)	含税单价(元/月)	含税合价(元)
1	C/S 应用代理系统	北京迅安 中盾 ZD-DP4 020	247685367622	2023-6-5	24	692	16608
2	C/S 应用代理系统	北京迅安 中盾 ZD-DP4 020	247685367646	2023-6-5	24	692	16608
3	移动 VPN 接入网关	北京迅安 中盾 ZD-VPN-G2000	247685367615	2023-6-5	24	692	16608
4	移动 VPN 接入网关	北京迅安 中盾 ZD-VPN-G2000	247685367592	2023-6-5	24	692	16608
5	B/S 应用代理系统	北京迅安 中盾 ZD-GLD L4020	228004637950	2023-6-5	24	692	16608
6	集中监控与审计系统	北京迅安 中盾 ZD-CMS	247685359405	2023-6-5	24	690.67	16576
7	B/S 应用管理	北京迅安 中盾 ZD-GLD	228004637803	2023-6-5	24	692	16608

	系统	L4020					
8	鉴别评估管理系统	北京迅安 中盾 ZD-RA4020	327102901036	2023-6-5	24	691	16584
9	身份认证管理中心	北京迅安 中盾 ZD-SRQ15-PD10	327100401401	2023-6-5	24	691	16584
10	移动 VPN 接入网关	北京迅安 中盾 ZD-VPN-G4020	311102502117	2023-6-5	24	692	16608
11	安全隔离网闸	天行网安 TG9255	WE3U2003180001	2023-11-19	18	1000	18000
12	安全隔离网闸	天行网安 Topwalk-GAP V3.0	LK-7612070037	2023-6-5	24	1000	24000
13	安全隔离网闸	天行网安 TG7109	YWE76141206	2023-6-5	24	1000	24000
14	集控探针	天行网安 TZ-2	YWE500940111	2023-6-5	24	1000	24000
15	安全视频交换系统	天行网安 TMS3000	WZ2014010127	2023-6-5	24	1000	24000
16	安全隔离网闸	天行网安 TG-10009-G	YWE80140103	2023-6-5	24	1000	24000
17	安全视频交换系统	天行网安 UMS3000	WZ2014010124	2023-6-5	24	1000	24000
18	集控探针	天行网安 TZ-2	YWE500930414	2023-6-5	24	1000	24000
19	安全视频交换系统	天行网安 TMS3000	WZ2014010125	2023-6-5	24	1000	24000
20	安全隔离网闸	天行网安 TG-10009-G	YWE80140101	2023-6-5	24	1000	24000
21	安全视频交换系统	天行网安 UMS3000	WZ2014010128	2023-6-5	24	1000	24000
22	集控探针	天行网安 TZ-2	YWE500940110	2023-6-5	24	1000	24000
23	安全隔离网闸	天行网安 TG-10009-G	YWE80140104	2023-6-5	24	1000	24000
24	安全视频交换系统	天行网安 UMS3000	WZ2014010126	2023-6-5	24	1000	24000
25	安全视频交换系统	天行网安 TMS3000	WZ2014010121	2023-6-5	24	1000	24000
26	安全隔离网闸	天行网安 TG-7259-G	YWE76131210	2023-6-5	24	1000	24000
27	安全数据交换系统	天行网安 UAS2000	WZ2014010134	2023-6-5	24	1000	24000
28	安全数据交换系统	天行网安 TAS2000	WZ2014010133	2023-6-5	24	1000	24000
29	安全数据交换系统	天行网安 UAS15009	WZ-R161219003	2023-6-5	24	1000	24000
30	安全数据交	天行网安 TAS15009	WZ-R161219002	2023-6-5	24	1000	24000

	换系统						
31	安全隔离网 闸	天行网安 TG-15009-G	LK-7612070004R	2023-6-5	24	1000	24000
32	安全数据交 换系统	天行网安 TAS15009	WZ-R161219007	2023-6-5	24	1000	24000
33	安全隔离网 闸	天行网安 TG-15009-G	LK-7612070003R	2023-6-5	24	1000	24000
34	安全数据交 换系统	天行网安 UAS15009	WZ-R161219008	2023-6-5	24	1000	24000
35	集控探针	天行网安 Topwalk/TZ- 1	WERT491122954	2023-11-19	18	1000	18000
36	安全隔离网 闸	天行网安 Topwalk/TG- 16089	WEW3U91128001	2023-11-19	18	1000	18000
37	安全数据交 换系统	天行网安 Topwalk/DTP -16089	WERT491122955/W ERT491122956	2023-11-19	18	1000	18000
38	安全数据交 换系统	天行网安 TAS15009	LEX-R1703210604	2023-6-5	24	1000	24000
39	安全隔离网 闸	天行网安 TG-15009-G	LEX-W1706140066R	2023-6-5	24	1000	24000
40	安全数据交 换系统	天行网安 UAS15009	LEX-R1703210617	2023-6-5	24	1000	24000
41	安全视频交 换系统	天行网安 TMS10009	LEX-R17032110570	2023-6-5	24	1000	24000
42	安全隔离网 闸	天行网安 TG-10009	LX-W170307060R	2023-6-5	24	1000	24000
43	安全视频交 换系统	天行网安 UMS10009	LEX-R1703210569	2023-6-5	24	1000	24000
44	安全视频交 换系统	天行网安 UMS3000	WZ2014010120	2023-6-5	24	1000	24000
45	安全隔离网 闸	天行网安 TG-10009-G	YWE80140105	2023-6-5	24	1000	24000
46	安全视频交 换系统	天行网安 TMS3000	WZ2014010129	2023-6-5	24	1000	24000
47	安全隔离网 闸	天行网安 TG-10009-G	YWE80140102	2023-6-5	24	1000	24000
48	安全视频交 换系统	天行网安 UMS3000	WZ2014010130	2023-6-5	24	1000	24000
49	安全视频交 换系统	天行网安 TMS3000	WZ2014010122	2023-6-5	24	1000	24000
50	集控探针	天行网安 TZ-I	LK-D1701100088	2023-6-5	24	1000	24000
51	安全数据交 换系统	杭州合众 DC-310-HS-HZ	NT00414830 (2-1)	2023-11-19	18	1000	18000
52	安全数据交	杭州合众	NT00414830 (2-2)	2023-11-19	18	1000	18000

	换系统	DC-310-HS-HZ					
53	请求服务系统	杭州合众 AS-310-HS-DZ	NT00414829 (2-2)	2023-11-19	18	1000	18000
54	请求服务系统	杭州合众 AS-310-HS-DZ	NT00414829 (2-1)	2023-11-19	18	1000	18000
55	请求服务系统	杭州合众 AS-300	NT00414828 (2-2)	2023-11-19	18	1000	18000
56	请求服务系统	杭州合众 AS-300	NT00414828 (2-1)	2023-11-19	18	1000	18000
57	安全单向光闸	杭州合众 SG-390	PR2510n201111254 2/PR2510n2011112 536	2023-6-5	24	1000	24000
58	安全单向光闸	杭州合众 SG-390	PR2510n201111254 1/PR2510n2011112 546	2023-6-5	24	1000	24000
59	安全数据交换系统	杭州合众 DC-390	H2015092202SG/H z2015092201SG	2023-6-5	24	1000	24000
60	安全单向光闸	杭州合众 SG-350	PR2510n201610241 /PR2510n20161024 2	2023-6-5	24	1000	24000
61	请求服务系统	杭州合众 AS-390	PR2510n201610243 /PR2510n20161024 4	2023-6-5	24	1000	24000
62	防火墙	启明星辰 USG-NGFW-P90	NT00419346	2023-11-19	18	1000	18000
63	防火墙	天融信 NGFW4000-UF	Q1611488075	2023-6-5	24	1000	24000
64	负载均衡	ARRAY 2600	1651M0486	2023-6-5	24	1000	24000
65	负载均衡	ARRAY 2600	1720M0688	2023-6-5	24	1000	24000
66	防火墙	天融信 NGFW4000-UF	K1103064508	2023-6-5	24	1000	24000
67	防火墙	网御星云 power v6000-u2000	NT00255509	2023-6-5	24	1000	24000
68	防火墙	网御星云 power v6000-u2000	NT00255508	2023-6-5	24	1000	24000
69	防火墙	天融信 NGFW4000-UF (NG-51228)	Q1711609159	2023-6-5	24	1000	24000
70	VPN	华三 NS-SecPath F1005	219801A0X0916CQ0 0267	2023-6-5	24	1000	24000
71	VPN	天融信 TopVPN 6000(TV-41606)	Q1811760535	2023-6-5	24	1000	24000
72	防火墙	启明星辰 USG-FW-12000E	819011312239997	2023-6-5	24	1000	24000
73	防火墙	启明星辰 USG-FW-12000E	819011202249999	2023-6-5	24	1000	24000

74	防火墙	启明星辰 USG-FW-12000E	819011212259997	2023-6-5	24	1000	24000
75	可信边界接入网关	中宇万通 TrustMore3600	SG24000201710110 01	2023-6-5	24	1000	24000
76	防火墙	启明星辰 万兆防火墙	NT00235391	2023-6-5	24	1000	24000
77	防火墙	网御星云 PowerV6000-F8310	NT00378035	2023-11-19	18	1000	18000
78	防火墙	华为 USG6550-AC	210235867110GC00 0582	2023-6-5	24	1000	24000
79	漏洞扫描	网御星云 TS-SC-E2700	NT00377834	2023-11-19	18	1000	18000
80	入侵检测	网御星云 TD3000-GS4000	2016231912179990	2023-11-19	18	1000	18000
81	安全日志审计	网御星云 Leadsec-RS-500	NT00377720	2023-11-19	18	1000	18000
82	防火墙	网御星云 PowerV6000-F8310	NT00378034	2023-11-19	18	1000	18000
83	防火墙	天融信 TG-60000	Q1705542577	2023-6-5	24	1000	24000
84	防火墙	华为 USG6000	210235867110GB00 0027	2023-6-5	24	1000	24000
85	防火墙	启明星辰 FW-1008DP	NT00215751	2023-6-5	24	1000	24000
86	防火墙	启明星辰 FW-1008DP	NT00215757	2023-6-5	24	1000	24000
87	链路负载均衡	深信服 AD-2000	5071004448	2023-6-5	24	1000	24000
88	链路负载均衡	深信服 AD-2000	5071004450	2023-6-5	24	1000	24000
89	入侵检测	启明星辰 NT600-TC-S	LSBJF14030126	2023-6-5	24	1000	24000
90	防火墙	启明星辰 USG-FW-12600GP	NT00237884	2023-6-5	24	1000	24000
91	防火墙	启明星辰 USG-FW-12600GP	NT00237886	2023-6-5	24	1000	24000

2、基础软件清单（提供原厂维保服务）

序号	软件名	数量	过保时间	维保期限（月）	含税单价（元/月）	含税总价（元）
1	公安应用日志安审系统	1	2023-6-5	24	1000	24000
2	e盾安全网络管理系统	1	2023-6-5	24	5500	132000

本合同金额为人民币大写：**贰佰壹拾柒万元整**，小写：**¥2170000.00**。

本次维保范围内的各类软硬件发生故障后，因修复产生的所有费用均包含在本项目中，不再另行计费。

项目的具体服务要求见集中采购机构的招标文件。

二、合同文件

下列文件是构成合同不可分割的部分，并与本合同具有同等法律效力，这些文件包括但不限于：

1. 常采竞磋[2023]0044号招标文件。
2. 乙方提交的投标文件。
3. 乙方投标的其他资料及承诺。
4. 评标记录。
5. 附件：科技信息化运行维护类项目交付物清单

三、质量保证

乙方所提供的服务必须符合国家有关标准和常州市公安局 2023 年度安全设备维保项目（常采竞磋[2023]0044号）的要求。

故障更换的配件需为原厂全新配件；含硬盘不返还服务。

四、服务时间

自合同签订之日起算，为期 2 年。

五、付款方式

合同签订，在收到发票后 15 个工作日内首付合同总价的 10%，即人民币贰拾壹万柒仟元整（¥217000.00）；服务满半年，在收到发票后 15 个工作日内支付至合同总价的 20%，即人民币肆拾叁万肆仟元整（¥434000.00）；服务满一年后，以合同总价的 20%为基础根据考核情况支付本款项；服务满一年半，在收到发票后 15 个工作日内支付至合同总价的 20%，即人民币肆拾叁万肆仟元整（¥434000.00）；服务满两年后，根据考核情况，在收到发票后 15 个工作日内根据考核情况支付余款。

六、服务要求

1. 运维管理

1.1 设备管理

乙方应为甲方建立规范化的信息系统基础信息管理维护体系，对设备档案信息、配置信息进行日常维护，保证系统基础运维资料的准确。

乙方在中标后，需在签订合同后一个月内对所维保的设备进行全

面排查，建立和完善信息台帐：包括设备的资产、位置、状态等全生命周期信息，设备拓扑结构图等并进行统一登记，建立完整的设备档案。对各类重要设备系统配置文件等进行备份，并以光盘刻录的形式提交。

1.2 巡检要求

巡检指标要求：

维保软硬件需做到无故障时间率不小于 99.5%。

$$\text{无故障时间率} = \frac{\text{软硬件无故障时间}}{\text{总运维时间}}$$

巡检频率要求：

(1) 每天一次例行巡检，检查设备是否正常运行，检查设备是否正常运行，有否异常情况（如异常声音、故障灯亮起等）；边界业务是否正常，配置策略是否生效等，对发现的问题及时报修处理，具体见“1.3、巡检内容”部分。

(2) 每月一次全面巡检，要求对设备运行状态、开通的业务、安全策略、安全风险等内容进行巡检。运维每满一个月，须在期满后三个工作日内出具详细的关于维保软硬件健康检查的《X 月巡检报告》。运维每满半年，须在期满后三个工作日内由资深工程师出具一次全面深度检查，并出具《半年巡检报告》。

(3) 法定节假日期间、重大活动（由甲方指定并提前告知）前及其举行期间，应根据甲方的具体要求对维保软硬件进行额外的巡检维护，确保在此时期的正常工作。

(4) 服务年度期满前十天完成年度现场维护，出具《年度服务总结报告》。在报告中需要提供年度的主要故障次数统计、系统性能评估报告、系统维护建议及日常故障处理的报告单等。

要求每次设备巡检、软件升级、硬件维修等工作均做好日记记录，形成管理台账。

1.3 巡检内容：

检查安全设备是否正常运行，是否有指示硬件故障报警；检查操作系统，通过查看系统日志等方式分析判断系统的运行状况；检查安

全设备文件系统、日志状态；检查 CPU、内存、磁盘、网络等的使用情况，记录异常信息。

（1）边界设备

边界设备包括天行网安、杭州合众的交换系统、单向光闸、网闸、集控系统及集控探针、可信认证网关等有线边界设备，以及北京迅安的 C/S 应用代理系统、移动 VPN 接入网关、鉴别评估管理系统、身份认证管理中心等无线边界设备。

检查设备是否正常运行，有否存在异常情况（如风扇异常声音，硬盘故障灯亮起等、电源模块蜂鸣）；是否有硬件故障报警。检查边界平台相关设备的 CPU、内存、硬盘使用率，性能是否存在瓶颈，配置是否正常，有无安全隐患，并做好相关巡检记录。

检查边界通道业务是否正常，检查数据交换是否正常，是否存在资源连接中断，业务数据积压，数据写入报错等问题，视频交换业务是否存在上下级网关不在线，视频流无法调取等问题，请求服务及授权访问业务是否存在业务无法正常请求与访问的问题，检查集控信息与上级节点通信是否中断等。

检查移动 VPN 接入网关配置代理策略，完成前置机 IP 地址及端口映射；网闸配置到映射到公安网地址；C/S 应用代理系统配置数据源、数据目标；鉴别评估管理系统警员证书签发、注销、延期等工作。定期查看集中监控及探针设备状态信息、业务流量使用信息、警员在线状态等。

按甲方要求配置、调整、删除边界通道资源，及时处理并上报业务故障，保证数据、视频交换及传输正常，对故障设备按照要求及时维修。

（2）防火墙、漏洞扫描

乙方每日检查设备是否正常运行，有否存在异常情况（如风扇异常声音，硬盘故障灯亮起等、电源模块蜂鸣）；是否有硬件故障报警。检查防火墙、漏洞扫描设备的 CPU、内存、硬盘使用率，性能是否存在瓶颈，配置是否正常，有无安全隐患，并做好相关巡检记录。

乙方按照甲方需求配置（或调整）防火墙、漏洞扫描的策略，故

障维修。每日查看安全策略日志，确认是否有网络攻击或渗透测试，定期汇总策略日志，整理成相关报告提交甲方，针对报告提出相关策略优化建议，对甲方要求的防火墙、漏洞扫描进行病毒库和特征库升级。

(3) 负载均衡

检查设备是否正常运行，有否异常情况（如风扇异常声音，硬盘故障灯亮起等）；是否有硬件故障报警。检查性能是否存在瓶颈，配置是否正常，有无安全隐患，并做好相关巡检记录。

乙方按照甲方需求配置、调整设备策略、故障维修。能够按甲方要求配置负载资源池，并保证已有负载池运行正常。

(4) 其他维保清单内的安全设备

检查设备是否正常运行，有否异常情况（如风扇异常声音，硬盘故障灯亮起等）；是否有硬件故障报警。检查性能是否存在瓶颈，配置是否正常，有无安全隐患，并做好相关巡检记录。

乙方按照甲方需求配置、调整设备策略、故障维修。并根据安全策略，定期汇总策略日志，整理成相关报告提交甲方，针对报告提出相关策略优化建议。

(5) 移动专网安全设备

对常州公安移动专网安全设备进行日常维护、发现并及时上报故障，按照甲方要求进行业务配置、调整等工作，包括 AAA 认证设备的用户配置、管理，网络接入控制器设备白名单设置、全局配置，网络探针、数据探针的监控配置、探针配置等工作。同时，配合进行常州市公安局移动警务证书的制发、注销，台账管理等工作。

常州公安移动专网安全设备清单：

序号	设备名称	设备品牌	设备型号
1	AAA 认证设备	一所中盾	ZD-AAA
2	网络控制器	一所中盾	ZD-TSSG
3	网络探针	一所中盾	ZD-MCA
4	数据探针	一所中盾	ZD-DC

1.4 业务维护

按照甲方要求提供软硬件稳定使用、新业务开通对接调配、已有

业务运行维护与流量监测、故障业务节点定位与协助排查、变更业务按需迁移割接、废止业务及时拆除服务等。

根据甲方应用或管理的需求，及时提供配置调整优化建议方案，获得甲方认可后，及时实施配置调整。针对安全设备日志采集需求，在本次维护服务期限内，乙方应免费完成本次维保项目内边界接入平台相关链路信息及业务信息与省厅“慧安”平台、常州市局大数据应用安全审计平台的对接工作。

维护服务期限内，遇到软件相关的日常维护及安装等问题，乙方在维护系统稳定运行的同时，主动收集系统关键补丁，软件补丁等信息，对安全产品的记录进行审计，对出现的安全隐患提出解决方案，在甲方的监督下，对业务系统实施升级服务，并在升级完成后配合甲方对系统进行测试和调优。

维护服务期限内，甲方如需对第三方软件或系统进行测试、调整或故障处理，乙方工程师应给予现场协助。

按甲方要求提供软件升级服务，在本次维护服务期限内，提供软件产品免费升级以及漏洞修复等服务。

按甲方要求提供以下安全设备的病毒库、特征库升级。

序号	设备类型	型号	序列号	基本情况	采购价	采购时间	过保时间	机房位置
1	防火墙	启明星辰 USG-NG FW-P90	NT00 4193 46	4个万兆接口，网络吞吐量40G，并发连接数460万	3800.00	2019-12	2023-1-19	市局信息中心机房
2	防火墙	天融信 NGFW4000-UF	Q161 1488 075	万兆设备，6个万兆光口，4个千兆电口。	2000.00	2016-3-0	2023-6-5	市局信息中心机房
3	防火	网御星云	NT00 2555	12个千兆电口，6个千兆SFP接口，配置2个千兆单模10km模块；吞吐量6Gbps，最大并发	1796	2015	2023	市局

	墙	power v6000- u2000	09	连接数 220 万，防病毒吞吐率 200Mbps，IPS 吞吐率 800Mbps，加解密吞吐率 200Mbps，IPSEC 最大隧道数无限制	8. 75	-1 2- 31	-6 -5	信息中心 机房
4	防火墙	网御星 云 power v6000- u2000	NT00 2555 08	12 个千兆电口，6 个千兆 SFP 接口，配置 2 个千兆单模 10km 模块；吞吐量 6Gbps，最大并发连接数 220 万，防病毒吞吐率 200Mbps，IPS 吞吐率 800Mbps，加解密吞吐率 200Mbps，IPSEC 最大隧道数无限制	17 96 8. 75	20 15 -1 2- 31	20 23 -6 -5	市局信息 中心机房
5	防火墙	天融信 NGFW40 00-UF (NG-5 1228)	Q171 1609 159	标准 2U 机箱，6 个 10/100/1000M Base-TX 接口，12 个 combo 接口（或者千兆电口 ≥ 4 且千兆光口 ≥ 12），冗余双电源；整机吞吐率 (bps)：12G；最大并发连接数：400 万；每秒新建连接数：10 万	10 00 00 .0 0	20 16 -1 1- 25	20 23 -6 -5	市局信息 中心机房
6	防火墙	启明星 辰 USG-FW -12000 E	0819 0113 1223 9997	2 个万兆光口 12 千兆电	21 60 00 .0 0	20 13 -1 -2 9	20 23 -6 -5	大数据 中心机房
7	防火墙	启明星 辰 USG-FW -12000 E	0819 0112 0224 9999	2 个万兆光口 12 千兆电	21 60 00 .0 0	20 13 -1 -2 9	20 23 -6 -5	大数据 中心机房
8	防火墙	启明星 辰 USG-FW -12000 E	0819 0112 1225 9997	2 个万兆光口 12 千兆电	21 60 00 .0 0	20 13 -1 -2 9	20 23 -6 -5	市局信息 中心机房
9	防火墙	启明星 辰 万 兆防火 墙	NT00 2353 91	万兆防火墙	20 00 00 .0 0	20 17 -3 -1	20 23 -6 -5	市局信息 中心

									机房
10	防火墙	网御星云 PowerV 6000-F 8310	NT00 3780 35	3个扩槽位, 6个万兆 SFP+插槽; 默认1个 10/100/1000M Base-TX; 并发连接数 400 万;	25 95 30 .0 0	20 20 -1 -1 5	20 23 -1 1-	19	大数据中心机房
11	防火墙	华为 USG655 0-AC	2102 3586 7110 GC00 0582	8GE 电+4GE 光, 支持电口 Bypass 卡, 4G 内存, 1 交流电源	28 80 0. 00	20 17 -9 -1 0	20 23 -6 -5		大数据中心机房
12	防火墙	网御星云 PowerV 6000-F 8310	NT00 3780 34	3个扩槽位, 6个万兆 SFP+插槽; 默认1个 10/100/1000M Base-TX; 并发连接数 400 万;	25 95 30 .0 0	20 20 -1 -1 5	20 23 -1 1-	19	大数据中心机房
13	防火墙	天融信 TG-600 00	Q170 5542 577	32个 10/100/1000Base-T 接口, 8个 SFP+插槽	27 93 00 .0 0	20 17 -9 -1 0	20 23 -6 -5		大数据中心机房
14	防火墙	启明星辰 FW-100 8DP	NT00 2157 57	配置 18 个千兆路由接口 6 个千兆电口 6 个千 兆光口 (含模块)。	11 30 00 .0 0	20 14 -9 -1 7	20 23 -6 -5		市局信息中心机房
15	防火墙	启明星辰 FW-100 8DP	NT00 2157 51	配置 18 个千兆路由接口 6 个千兆电口 6 个千 兆光口 (含模块)。	11 30 00 .0 0	20 14 -9 -1 7	20 23 -6 -5		市局信息中心机房
16	防火墙	启明星辰 USG-FW -12600	NT00 2378 84	标准 2U 设备, 双冗余电源; 标配 6 个 10/100/1000M Base-TX 接口, 5 个扩展槽位;	17 00 00 .0	20 16 -1 0-	20 23 -6 -5		市局指挥

		GP			0	30		中心机房
17	防火墙	启明星辰 USG-FW-12600 GP	NT00 2378 86	标准 2U 设备, 双冗余电源; 标配 6 个 10/100/1000M Base-TX 接口, 5 个扩展槽位;	17 00 00 .0 0	20 16 -1 0- 30	20 23 -6 -5	市局指挥中心机房

1.5 服务授权

维保清单中第 81 项安全日志审计设备 (型号: 网御星云 Leadsec-RS-500 序列号: NT00377720), 新增 70 个审计对象授权。

1.6 其他要求

按甲方要求提供加强服务, 在重大安保任务、敏感时间节点、业务迁移等期间, 能够根据业务需要另外安排工程师提供加强服务。

按甲方要求负责所维保设备的上下架、迁移、搬迁等工作及软件重新部署等工作, 如该变更工作是其他项目内容, 乙方须配合完成所维保设备所在相关系统其它硬件设备的上下架、迁移、搬迁等工作及软件重新部署等工作。

本项目维保期内, 甲方业务系统遇到严重故障时, 提供能够满足业务运行要求的各种设备进行临时替换。

2. 故障处理

2.1 服务响应要求

(1) 服务响应及维修。提供 7*24 小时的技术支持和服务。5 分钟内对甲方所提出的需求做出响应, 1 小时内到达现场, 承诺在规定的时间内完成维修。

(2) 故障响应及恢复。

按故障严重程度从高到低分为四级:

重大故障: 核心业务系统不可用或将导致其业务数据缺失的;

严重故障: 核心业务系统性能受到严重影响的故障或可能导致核心业务系统不可用的, 非核心业务系统不可用的或导致其业务数据缺失的;

较大故障：非核心业务系统性能受到严重影响的故障或可能发生严重以上故障风险的故障；

一般故障：其他隐患类故障。

要求做到全天候 7*24 小时的技术服务，对于故障抢修涉及的响应时间和故障处置时间的要求如下：

故障响应。

(a) 重大及严重故障：故障发生后，应在 5 分钟内人员响应，30 分钟内到达故障服务现场。

(b) 较大及一般故障：故障发生后，维修人员到达故障服务现场的时间应不大于 1 小时，具体为：工作时间维修人员到达故障服务现场的时间应不大于 30 分钟，非工作时间维修人员到达故障服务现场的时间应不大于 1 小时。

故障恢复。

重大故障：恢复时间在工作时间内不超过 1 小时，非工作时间内不超过 2 小时；

严重故障：恢复时间在工作时间内不超过 2 小时，非工作时间内不超过 3 小时；

较大故障：恢复时间不超过 4 小时；

一般故障：其他隐患类故障，恢复时间由乙方与甲方协商决定，原则上不超过 1 工作日。

重大、严重故障连续发生一个月内两次以上的，除提交故障处置报告以外还应提交问题分析报告，深度分析故障产生的原因，并提出预防性改善建议。

(4) 如因特殊原因无法在指定处置时间内修复故障的，乙方需将故障原因、过渡方案和恢复计划等在 2 小时内书面上报，并在此期间积极配合相关应用开发商实施过渡方案，全力保证应用的不间断，临时过渡方案产生的人力成本、时间成本、社会经济损失等由乙方承担。

(5) 在重大、严重故障或者甲方要求提供故障报告的故障处理结束后 24 小时内应向甲方提出书面故障处理报告。

(6) 乙方在本次所维保设备发生故障无法排除的情况下，乙方须协调原厂解决，所涉及的费用由乙方承担。

2.2 备件服务要求

建立备件库，为保证系统故障时快速响应，本次要求乙方提供常用设备及配件作为本次项目备件。

常用配件存放于甲方处，具体清单如下（不少于以下清单）：万兆数据交换平台 1 套、万兆视频网闸 1 套、请求服务系统 1 套、安全单向光闸 2 套，相关设备须符合公安部边界平台技术标准，所有更换的备件必须为原厂生产且可正常运行，以保证甲方系统的安全、可靠、稳定运行。乙方需保证涉及维保设备的硬件都能够得到及时、准确的维修。

如遇配件供给时间或故障问题复杂导致解决时间超过 24 小时，必要时需提供备机以保证业务系统正常运转。

在运维过程中，需根据维保情况，经甲方同意，对备件库进行更新，保证备件匹配。

2.3 其他要求

维保单位应配备日常维护、应急抢修必须的维护终端、网线钳、工具包、标签机、检测工具等设备，并免费提供维保所需相关耗材。上述设备应为本维保项目专用，需保证设备性能良好，乙方不得以任何借口挪用相关设备。

负责对市局不在本次维保范围内的安全设备，总数约十余台，进行台账梳理、日常巡检、维护和维修（需进行硬件更换时，由甲方提供硬件）。

乙方应自行建立安全体系，并承担安全事故造成的一切责任，甲方对此不承担连带责任。

3. 维护人员

3.1 乙方须配备 1 名专业工程师提供两年 5*8 小时驻场服务，驻场人员要求及工作职责如下：

技能要求：3 年以上安全运维相关工作经验；熟悉网络安全相关的安全体系和运营流程，具有网络安全项目实施与维护经验；熟悉各

主流网络安全产品的工作原理、功能与运维操作，如下一代防火墙、WAF、IPS、防病毒管理、漏洞管理、威胁情报、安全态势感知等产品操作技能；具有丰富的网络安全应急响应和处置经验，具备安全事件溯源能力，以及独立的分析和解决问题能力；具有边界接入平台建设、产品实施和维护及相关工作经验。

工作职责：

（1）日常运维

驻场工程师每天对维保设备进行日巡检，并在蓝海平台上提交日巡检报告，每月提交一次月度巡检报告，每半年提交一次半年技术服务报告。驻场工程师在维护工作中，有义务对代维设备作好标签制定、技术文件入档编辑、配置版本的保留和归档、软件版本的保留和归档、线缆的整理等，驻场工程师在现场进行维保软硬件设备管理和监测，及时排查故障，对需要调整的配置经授权同意后进行修改，驻场工程师须负责把需要乙方出面处理的事务信息及时反馈到乙方，解决代维的设备维修以及厂商的技术及设备的配合。

针对各类边界包括感知网到公安网视频数据边界、党政军数据边界、企事业数据边界、社会信息采集数据边界、无线接入边界、二类区到公安网视频边界、互联网到二类区视频边界、互联网到感知网数据边界、PDT 专网到公安网边界、社会面接入共享网到感知网视频边界、地铁专网到感知网等边界，配合完成运行业务的统计巡检、新业务的配置对接、旧业务的清理撤除、业务台账梳理以及故障业务的排查诊断。

（2）故障处理

对发生的突发事故，在接到故障响应需求后 5 分钟内到现场（非工作日 1 小时内到达），服务内容包括对意外事故的处理，非法入侵的处理和调查恢复、网络攻击的应急防护等。对边界安全交换系统的软硬件提供现场维护。

当设备出现硬件故障需要维修时，驻场人员应联系相关厂商，上门下架故障设备，保内设备将直接发送报修，维修后进行恢复性安装，并做好配置。若所维保的设备发生故障需要更换配件时，对于一般不

影响工作的故障，一般配件当天供应，特殊配件 2 天内供应，对于影响正常工作的故障，应于 24 小时内排除，无法及时修复的，应提供备机或备件服务，不在该项目维保范围之内损坏的物品，器件则另行协商收费。

（3）安全服务

驻场工程师每日做好所维保安全设备的安全监测，如发现渗透攻击、病毒传播等安全事件，需立即处置，第一时间消除安全风险隐患。

驻场工程师根据所维保安全设备安全监测情况，收集、汇总安全态势情况，形成安全态势月报。

驻场工程师需协助甲方消除安全风险隐患，针对公安部、省厅、市委网信办下发的及市局自行发现的系统漏洞等安全风险隐患，提出整改建议并协助完成整改。

3.2 乙方须承诺保持驻场工程师的连续性和稳定性。人员调整更换必须经甲方同意，中途更换人员需提前一个月告知甲方，待甲方批准后方可更换，以正式函件送达甲方并由甲方签字确认为准，更换的人员必须具有同等档次，更换驻场工程师需根据岗位情况至少保证两周的工作交接期，保证甲方系统维护稳定性。

3.3 驻场工程师食宿自理，自行准备维护终端（维护期满后，硬盘不返还），驻场人员的工作的时间由甲方负责安排，包括正常工作时间、周末、节假日或夜间加班值班；驻场人员工作的所有费用（包括工资、因甲方工作安排产生的差旅费、加班费等）由乙方承担。

3.4 乙方必须符合甲方相关工作规范要求，驻场人员应按照甲方管理要求进行日常工作。驻场工程师考核由甲方负责，服从甲方的管理，包括工作时间、工作安排，严格执行请销假制度，在服务期内不得兼任其他项目的维护工作。

技术支持团队

乙方须建立与本项目相符的后台技术支持团队，后台技术支持团队人员需相对固定，并在发生现场驻场人员无法处理故障时，第一时间赶到，不得推诿。

4. 原厂维保

为确保市局核心业务运行正常，本项目中明确要求或者乙方承诺提供原厂维保的，乙方须保证原厂商为代维设备及软件至少免费提供以下服务：

天行网安设备、北京迅安设备：

每月现场巡检，对设备运行状态、开通的业务、安全策略、安全风险等内容进行巡检，并做好记录，形成管理台账。

提供 7*24 热线电话支持服务，提供不限时间、不限数量的售后电话支持，在发生故障 5 分钟内电话响应，6 小时内解决问题，如不能解决，在 8 小时内安排原厂商高级技术人员到达现场，12 小时内解决问题，如不能解决，在 48 小时内提供备件。

提供软件升级服务，在本次维保项目质保期内，根据甲方要求提供软件产品免费升级服务。

公安应用日志安审系统：

平台业务功能日常巡检服务。巡检内容包括平台门户、日志采集管理、日志查询、日志分析、监测预警、级联管理和系统管理各功能模块正常稳定，发生故障保证及时处置，保障安审平台正常运行正常。

根据甲方要求，对现有平台进行服务器迁移，确保迁移后平台业务正常，各功能模块正常稳定。

根据省厅要求，做好数据维护，保证系统运行正常率、日志更新率、日志规范率均达到 100%。

e 盾安全网络管理系统：

对公安信息网 e 盾安全网络管理系统进行软件升级，升级后需能在“一机两用”监控系统及公安网苏警盾前，发现并阻断违规外联；此次升级，还需在感知网同步部署一套不少于 2000 台终端授权的 e 盾安全网络管理系统，需能在感知网苏警盾前，发现并阻断违规外联。

系统业务功能日常巡检服务。巡检内容包括系统后台日志查询、日志分析、监测预警和系统管理各功能模块正常稳定，发生故障保证及时处置，保障 e 盾安全网络管理系统正常运行正常。

数据维护服务。包括平台日志查询、违规数据查询、用户访问策略管理、数据备份等维护服务等。

月度运维报告服务。要求每月向甲方书面提供月度运维报告，包括系统运行状态、客户端安装率、当月违规情况等内容。

半年度维护报告服务。要求提供半年度系统运行状态、违规情况统计报告。

七、保密要求

1. 按照公安机关要求，落实好企业、人员管理、备案工作。

2. 乙方保证其公司人员在服务期间所接触的甲方各种文件，数据，系统资料，系统操作等严格遵守甲方保密制度，不得向第三方透露。

3. 公安业务系统数据属于公安秘密，乙方应当严格遵守相关规定，严禁泄漏公安秘密，未经甲方确认，乙方的其公司人员不得对甲方业务系统作任何操作，参与项目维保人员必须做到以下几点：

只在规定的区域实行规定的工作，不得进入与之无关的工作区域；

不得在机房设备上建立与工作无关的网站、网页和服务；不得在设备中传输、粘贴有害信息或与工作无关的信息；

不得擅自对设备进行扫描、探测和入侵信息系统；

不得对工作信息和资源越权访问、违规使用；

不得私自允许他人接触和使用机房设备；

严禁将工作用设备和文件带离机房；

未经机房管理部门同意，严禁以任何方式和介质拷贝服务器上的任何信息及项目中涉及的信息；

对工作中接触到的信息做到保密；

不准擅自摘抄、下载、复制、拍摄、提供、销毁或私自留存相关文件、资料（含电子文档）；严禁违反“一机两用”规定；不准在私人交往中谈论相关工作；

不得有其他任何危害公安信息安全的行为。

4. 按照各级公安机关对公安信息网络的安全要求，由乙方与甲方签定安全保密协议，落实公安网络安全及信息保密的各项规定。乙方对驻场工程师必须进行相关安全保密教育，与甲方签订保密协议，有履行保密的责任和义务。

5. 凡以直接、间接、口头或书面等形式提供涉及保密内容的行为均属泄密，将追究当事人及维保单位的责任。

6. 项目结束后，所有资料全部移交给甲方。

八、考核要求

1. 考核办法。

维保服务质量实行按月定量考核制度，考核打分办法如下：

1.1 日常巡检服务（15分）

完全按照甲方规定的流程进行巡检（包括日巡检、月巡检、半年度巡检、年度巡检及甲方要求的巡检计划）的不扣分，发生一次未遵循规定流程巡检或者不巡检的，扣0.5分，发生2次的扣2分，发生3次的扣5分，超过3次的，本项分值扣为0分。

1.2 服务响应时限。（15分）

发生重大及严重故障在时，非工作时间内到达现场时间不超过1小时。（每迟10分钟扣1分，直到本月得0分）。

1.3 故障解决时限（30分）

重大及严重故障，修复时间不超过 2 小时，每超过 30 分钟扣 5 分，直至本月得分为 0 分。

较大故障，修复时间不超过 4 小时，每超过 1 小时扣 2 分，直至本月得分为 0 分。

一般故障，修复时间不超过 24 小时，每超过 1 小时扣 1 分，直至本月得分为 0 分。

因乙方操作失误导致所维保设备或其他相关设备出现故障，正常运行的业务受影响或者不可用，按照影响情况扣 1-10 分/次，直至本月得分为 0 分。

1.4 文档提交及时性。(20 分)

每日巡检报告(蓝海平台上午 10:00 点前提交，发生 1 次未按时提交的扣 1 分，直到本月得 0 分)。

提供每次维修可操作的详细步骤及应急方案。(每次维修当天提交，每迟 1 天扣 1 分，直到本月得 0 分)

故障报告。(每次故障后 2 天内提交，每迟 1 天扣 1 分，直到本月得 0 分)

月度服务报告。(次月 3 号前提交，每迟 1 天扣 1 分，直到本月得 0 分)

半年服务报告。(下半年首月 3 号前提交，每迟 1 天扣 2 分，直到本月得 0 分)

年度服务报告。(服务结束前 10 天内提交，服务结束后每晚 1 天扣 3 分，直到得 0 分)

1.5 驻场人员管理(20 分)

驻场人员须按照甲方要求正常上下班，

每出现 1 人/次迟到、早退扣 1 分，

每出现 1 人/半天旷工扣 5 分，

办公区域不整洁、着装不规范等发现 1 人/次扣 1 分，

未按时完成交办任务的每 1 人/次扣 1 分，

交办任务不执行或不完全执行扣每 1 人/次扣 1 分，

被所在部门或上级部门检查发现或通报的批评的，每 1 人/次扣 10 分，

中途更换驻场人员，驻场人员交接过程中内断档 1 天，按旷工 1 天计算，以此类推。

1.6 加分奖励（10 分）

开展技术培训，加 2 分。

主动服务并得到认可，加 2 分。

当月没有出现任何故障，加 2 分。

获得甲方书面表扬的，加 4 分。

本项加分上限为 10 分。

1.7 一票否决项（扣 100 分）

乙方触犯以下任意一条，甲方都可以执行一票否决。

（1）乙方发生违反保密协议的；

(2) 巡检及故障处理中违规操作，造成甲方设备损坏、数据丢失等严重后果的；

(3) 遇到设备故障，故意拖延处理，导致严重后果的；

(4) 在巡检报告、故障处理报告等文件中弄虚作假，情节严重的；

(5) 乙方在合同执行中有触犯法律法规的其他情形。

2. 月得分计算办法

每月扣分=故障响应时间+故障恢复时间+业务不可用时限+健康检查服务+文档提交及时性+一票否决项。(扣分原则是扣到本月得分为 0)。

每月得分最高 100 分。

3. 考核月得分表格:

序号	日常巡检服务	服务响应时限	故障解决时限	文档提交时限	驻场人员管理	加分奖励	一票否决项	合计
1								

维保期内，甲方有权根据实际情况对具体考核条款进行调整。

九、考核罚则

1. 每出现一次一票否决项，扣除合同总价的 3%，一个月内出现两次一票否决项，扣除合同总价的 10%。

2. 年度得分=月度得分之和/12，低于 95 分的，扣除合同总价的 5%。

3. 月度服务得分连续两个月低于 80 分的，甲方有权终止维保服务合同。

4. 乙方服务响应时间、更换硬件到达时间不达标，按以下规定进行赔偿：

合同签订 30 天内以及合同履行期内每季度，甲方不定期对乙方投标时的各项响应进行抽查，如发现不能满足响应的，每次扣除合同总价的 1%。核查项目包括：

(1) 对备品备件库抽查，甲方在乙方响应的备品清单中选择 1 个或者多个备件，要求乙方在标书承诺的备品备件到达时间内到达现场，根据备件序列号查询真伪。

(2) 对维保工程师团队抽查，甲方设置模拟故障演练，要求乙方按响应的维保工程师清单，安排维保工程师现场处理。

5. 因维保设备原因或乙方原因导致严重故障（分局范围网络瘫痪、部门性业务系统所有用户不可访问等），单次故障时间超过 4 小时的，每 4 小时扣除合同总价的 0.2%；因维保设备原因或乙方原因导致重大故障（全局网络瘫痪，全局性业务系统、对外窗口服务业务所有用户不可访问等），单次故障时间超过 2 小时的，每 2 小时扣除合同总价的 0.2%。一个月内连续出现 2 次以上两种情况的再扣除合同总价的 0.2%，出现第 3 次的甲方有权中止合同执行，并由乙方承担相应的经济及法律责任。

6. 乙方派驻的工程师未得到甲方认可或中途变更驻场工程师（未得到甲方确认），否则扣除合同总价的 2%。

7. 在维保存储设备出现磁盘损坏，乙方在处理故障时，造成数据丢失并导致数据资源不能恢复的严重情况甲方有权中止合同执行，并由乙方承担相应的经济及法律责任。

8. 系统设备发生故障后,在规定时间内无法解决技术问题和更新故障软硬件,直接影响甲方正常开展业务工作的,甲方有权选择第三方公司提供服务,所需费用由乙方承担。

9. 因维保设备原因或乙方原因对其他业务系统、设备造成影响,由乙方承担系统恢复、设备维修的所有费用,并承担由此造成的损失。

十、其他要求

1. 乙方应建立完整的文档记录,按时向甲方提供装订成册的纸质版与电子版,具体要求为:

(1) 签订维保合同 10 天内,乙方提交《系统日常巡检作业指导书》。《系统日常巡检作业指导书》经甲方审核、批准后,由常驻现场技术人员执行日常巡检;

(2) 签订维保合同 10 天内,乙方提交《维保设备信息登记表》,记录保修设备的详细配置信息;维保期及时维护和更新《维保设备信息登记表》,包括位置、参数、配置的变更;

(3) 签订维保合同 10 天内,乙方须提供本项目要求的原厂维保证明文件。在合同执行过程中,乙方应当提供原厂质保但未提供的,甲方有权解除合同,并追究乙方相关责任;

(4) 在维护过程中,乙方须提供至少以下交付物:《每日巡检单》、《X 月巡检报告》、《半年度巡检报告》、《年度巡检报告》、每次故障处理后的《故障解决报告单》、重大故障处理后的《重大故障处理分析报告》、根据巡检结果触发的《某一设备、系统优化调整方案》、甲方提出的《关于某一事项的咨询服务报告》、须原厂服务提供的《某设备的巡检报告》等,维护结束后须提供《年度服务总结报告》,在报告中需要提供年度的主要故障次数统计、系统性能评估报告、系统维护建议及日常故障处理的报告单等内容。年度报告作为年度付款依据。

2. 乙方须在甲方需要的情况下，无偿配合甲方进行应急演练、业务系统调整、升级等非故障性事务的处理。

3. 乙方执行过程中应按照《常州市公安局科技信息化运行维护类项目管理办法》按时提供运维台账、巡检日志、阶段性维护报告等运维过程资料。

4. 维保期间维保设备、配件、培训和服务不再收取任何其他相关费用，如配件费、维修费、劳务费、交通费、培训费等。

5. 乙方应服从甲方对管理维护工作的安排，接受第三方测试机构、监理单位、纪检监察等甲方指定机构的管理和质询。

6. 乙方为甲方提供操作维护培训，直至其能熟练独立操作设备及日常维护与保养，设备及业务系统简单故障诊断与排除。

7. 乙方应尽可能在满足本技术规范的基础上，在投标文件中提出更好的方案。招标文件中未提及的规范与标准，在系统维护中又确实需要的，乙方都应按照国家标准和行业标准以及相关工程的常规做法加以补充完善，保证系统及设备的性能完全符合本招标文件中关于系统技术规范的要求。

十一、违约责任

1. 如果甲方延期付款或者未尽配合义务，乙方不承担由此引起的项目建设工作的损失与责任，工期顺延；

2. 因乙方原因延误工期，乙方每延误 1 天按照合同总价的万分之五向甲方补偿延误费；

3. 保修期内乙方如果不能在合同规定的时间内作出反应和修复故障，每超出 1 天按合同总价的万分之五计算违约金。

4. 在合同执行过程中，乙方应当提供原厂质保但未提供的，甲方有权解除合同，并追究乙方相关责任。

十二、不可抗力

1. 在执行合同期限内，任何一方因不可抗力事件造成不能履行合同时，应立即通知对方，并寄送有关权威机构出具的证明，则合同履行期可延长，延长期与不可抗力影响期相同。出现上述情况甲乙双方不承担合同有关逾期违约责任。

2. 不可抗力影响时间持续 30 日以上时，甲乙双方均可以单方面解除合同。

3. 本条所述“不可抗力”是指不可预见、不能克服及不能避免的事件，包括战争、严重火灾、洪水、地震等。

十三、合同纠纷处理

1. 凡涉及本合同或因执行本合同而发生的一切争执，应通过协商解决。

2. 如果协商不能解决，则提交常州仲裁委员会进行仲裁。

3. 争议在处理过程中，除正在进行仲裁或诉讼的部分外，合同的其他部分将继续执行。

十四、其它约定事项

1. 如需修改或补充合同内容，应经甲、乙双方协商一致，共同签署书面修改或补充协议。该协议将作为本合同不可分割的一部分。

2. 除甲方事先书面同意外，乙方不得转让任何其应履行的合同义务。

3. 本合同未尽事宜，按中华人民共和国现行有关法律法规执行。

十五、合同生效

本合同经双方盖章签字后生效，如有变动，必须经双方协商一致后，方可更改。本合同一式肆份，甲方贰份，乙方壹份，集中采购机构壹份。


其他未尽事宜，参照相关法律，双方协商解决。

(此页无正文)


甲方(盖公章): 常州市公安局



乙方(盖公章): 江苏移动通信系统集成有限公司



法定代表人:

法定代表人: 

代理人:

代理人:

经办人:

电话: 010-82800016

电话:

开户银行: 中国银行南京云
锦路支行

银行帐号: 479361758530

附件：科技信息化运行维护类项目交付物清单

序号	服务目录	触发条件	交付物	备注	交付时效
巡检类					
1	日常巡检	每天	每日巡检记录	包括代维设备的电源、风扇、网络、故障指示灯等基本运行情况，核心数据库运行情况的巡检登记记录。 巡检记录在蓝海平台登记，不输出纸质材料。	工作日当天
2	月巡检	每月	每月巡检报告	包括资深工程师出具深度巡检报告（包括但不限于软硬件运行情况，存在风险及优化方案等内容），该月设备运行整体状况，维修记录等。 输出纸质报告，电子稿上传蓝海平台登记。	下一个月第三个工作日前
2	半年度巡检	每半年	半年度巡检报告	包括资深工程师出具深度巡检报告（包括但不限于软硬件运行情况，存在风险及优化方案等内容），该半年设备运行整体状况，维修记录等。 输出纸质报告，电子稿上传蓝海平台登记。	下一个月第三个工作日前
3	年度巡检	每年维护完成后	年度维护报告	需要提供本年度的主要故障次数统计、系统性能评估报告、系统维护建议及日常故障处理的报告单、设备除尘情况说明。 输出纸质报告，电子稿上传蓝海平台登记。	年度结束前第十个工作日前
故障处理类					
1	硬件故障响应	设备产生硬件故障	一般故障出具处理记录，重大故障出具故障报告	需包括事件发生情况、处理过程（硬件备件更换、软件日志文件分析、调试等）、系统恢复、影响程度等情况。 输出纸质报告，电子稿上传蓝海平台登记。	故障处理完成后第二个工作日前
2	软件故障响应	软件产生故障			故障处理完成后第二个工作日前
评估调优类					
1	磁盘空间整理	系统空间不足	系统调优申请、系统调优方案及调优报告	输出纸质报告，电子稿上传蓝海平台登记。	需求发生后一周内或要求时间内
2	日志文件分析	系统出现故障			
3	修补系统软件最新补丁	重大漏洞影响业务安全			

4	系统参数调整及性能优化	系统参数设置影响系统性能			
5	系统升级扩容咨询服务	原应用系统有升级扩容需求			
6	系统软件咨询服务	有需要时			
7	网络优化	网络优化			
注：所有纸质输出物须甲、乙、用户方（如有）多方签字。					