

项目编号：济源采购-2023-582

合同编号：JYZH-SR-2023-016

项目合同

项目名称：济源市行政服务中心电子政务运维与安全检查服务采购项目

甲方：济源市行政服务中心

乙方：河南济云智慧科技有限公司

签订时间：2023年11月29日

签订地点：河南省济源市

合同正文

甲乙双方根据《中华人民共和国民法典》和国家有关法律法规的规定，本着自愿平等、互利有偿和诚实信用的原则，就下述“济源市行政服务中心电子政务运维与安全检查服务采购项目”进行友好协商达成如下合同。

第一条 本合同服务内容与要求：

第一部分服务内容：电子政务运维服务

对济源市电子政务中心机房运维、对第二行政区一号楼信息化相关设备设施运维、对年度行政服务中心电子政务设备更新计划和方案编制等。

第二部分服务内容：电子政务信息系统安全检查服务

按照国家信息安全有关法规政策要求，对电子政务信息系统进行检查，掌握信息安全总体状况，发现存在的主要问题和薄弱环节，进一步健全信息安全管理制度，完善信息安全技术措施，提高信息安全防护能力。安全检查内容包括但不限于：信息安全组织管理、信息安全防护管理、信息安全应急管理、信息安全教育培训、信息安全整改工作等。

具体内容及要求见附件。

第二条 项目的服务期限为：一年，时间为：2023年12月3日至2024年12月2日。

第三条 服务地点：济源市行政服务中心要求的服务地点。

第四条 甲方应按以下方式支付运维费用：

1. 项目运维费用为【¥704,000.00（柒拾万零肆仟元整）】人民币。

2. 维护费用由甲方按照政府采购程序支付给乙方。具体支付方式和时间如下：

- 合同签订后，运维服务开始，乙方在合同签订后五个工作日内向甲方提供正规发票，甲方支付总合同款的50%作为预付款，即【¥ 352,000.00（叁拾伍万贰仟元整）】人民币。
- 服务期结束前，乙方向甲方提供正规发票后，甲方支付乙方总合同款剩余的 50%，即【¥352,000.00（叁拾伍万贰仟元整）】人民币。

第五条 双方确定因履行本合同应遵守的保密义务如下：

甲方：

1. 保密内容（包括技术信息和经营信息）：包括但不限于技术性信息、商业性信息、文件、程序、计划、技术、图表、数据、标准、专有技术、业务或业务运作方法以及其他专有信息，本合同的条款和与本合同有关的其他商业信息和技术信息。
2. 涉密人员范围：项目相关人员。
3. 保密期限：乙方运维期限内。
4. 泄密责任：按被泄密方损失赔偿。

乙方：

1. 保密内容（包括技术信息和经营信息）：包括但不限于技术性信息、商业性信息、文件、程序、计划、技术、图表、数据、标准、专有技术、业务或业务运作方法以及其他专有信息，本合同的条款和与本合同有关的其他商业信息和技术信息。
2. 涉密人员范围：项目相关人员。
3. 保密期限：乙方运维期限内。
4. 泄密责任：按被泄密方损失赔偿。

第六条 双方确定，按照招标要求对乙方完成的运维成果进行验收：满足项目用户招标文件、合同需求，通过终验后则视为通过验收。

第七条 双方确定：任何一方违反本合同约定，造成交付或付款工作停滞、延误或失败的，按以下约定承担违约责任：

1. 乙方运维服务中，如果系统发生不影响主业务运行的瑕疵或问题，不影响甲方系统正常使用，开始初验，同时乙方承诺在终验结束前解决这些瑕疵或问题。
2. 维护期结束后，如果因乙方原因，系统仍有不满足合同约定之需求的问题，则维护期延长，终验推迟直至问题解决。
3. 对于非乙方原因造成的问题，导致无法进行验收，双方应积极协商解决问题，任何一方故意拖延解决问题，则视为违约。
4. 如乙方未完全满足本项目的服务要求，或者不积极配合导

致项目无法正常运行，甲方有权单方面扣除该项目的部分经费。

5. 甲方按时支付款项，但不因财政支付流程延误而承担违约责任。

第八条 双方对运维约定如下：

1. 服务期限内每年度更换设备费用总额超过 30 万元时，超出部分由采购方承担。更换设备不足 30 万元时，由采购方指定更换需要更换的设备，更换设备的总数额需达 30 万元。更换设备清单由甲方负责审查；乙方提供的设备配件应是原厂配件；如有替代品，替代品的性能应不低于原产品性能，替代品须经甲方同意后方可替换。
2. 若甲方对乙方提供的服务比较满意，甲方可在服务期满后延续运维服务。

第九条 双方确定，在本合同有效期内，甲方指定谢学广为甲方项目联系人，乙方指定姚诗琪为乙方项目联系人。

项目联系人承担以下责任：保证甲乙双方联络沟通、配合对方要求，提供相关资料、监督合同的履行情况。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，应承担相应的责任。

第十条 双方确定，因发生不可抗力或技术风险，致使本合同的履行成为不必要或不可能的，双方应协商解决。

第十一条 双方因履行本合同而发生的争议，应本着公平合理的原则

协商解决；若协商不成，任何一方有权向乙方注册所在地的人民法院提起诉讼。

第十二条 双方确定：与履行本合同相关的投标文件、中标通知书，为本合同的组成部分。

第十三条 双方约定本合同其他相关事项为：

1. 未尽事宜双方本着长期合作的态度进行友好协商。
2. 甲方同意乙方将本案例列入乙方的成功案例列表，但乙方不得夸大宣传或直接将其运维方案、数据提供给其他机构或个人。

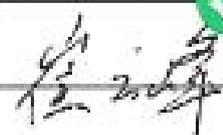
第十四条 本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

第十五条 本合同经双方签字盖章后生效。

附件：1、济源市行政服务中心电子政务运维与安全检查服务采购项目服务内容及要求

2、济源市行政服务中心电子政务运维与安全检查服务采购项目运维设备清单

甲方：  济源市行政服务中心  (盖章)
法定代表人/委托代理人： _____ (签名)
_____ 年 月 日

乙方：  河南张云智能科技有限公司  (盖章)
法定代表人/委托代理人  (签名)
_____ 年 月 日

附件 1:

济源市行政服务中心电子政务运维与安全检查服务 采购项目服务内容及要求

一、项目概况

本项目服务内容包含:

1. 提供电子政务运维服务: 对济源市电子政务中心机房运维、对第二行政区一号楼信息化相关设备设施运维、对年度行政服务中心电子政务设备更新计划和方案编制等;

2. 提供安全检查服务: 按照国家信息安全有关法规政策要求, 对电子政务信息系统进行检查, 掌握信息安全总体状况, 发现存在的主要问题和薄弱环节, 进一步健全信息安全管理, 完善信息安全技术措施, 提高信息安全防护能力。安全检查内容包括但不限于: 信息安全组织管理、信息安全防护管理、信息安全应急管理、信息安全教育培训、信息安全整改工作等。

二、服务内容及技术要求:

第一部分服务内容: 电子政务运维服务

(一) 电子政务运维服务内容

1. 市电子政务中心机房运维

1.1 现有市电子政务中心机房及软硬件设施的运维

1.1.1 业务系统、数据库、中间件, 包括所有正在使用的业务系统、数据库及中间件。业务系统包括业务系统的正常运行维护迁移和各软件的二次开发(定制开发)、系统间的整合优化等; 数据库包括

oracle、sqlserver、Mysql、DBII、access 等的运行维护调整优化迁移；中间件包括 weblogic、Tomcat、Apache 等的运维升级等。

1.1.2 主机系统，包括电子政务机房内所有的服务器；

1.1.3 存储系统，包括电子政务机房内所有的存储系统；

1.1.4 网络设备，包括电子政务网络所有的主干网络设备；

1.1.5 安全设备，包括电子政务机房所包含的安全设备；

1.1.6 其他设备设施，包括电子政务中心机房及电源机房所有显示器、光纤网线、UPS（包含配套电池）、KVM、消防、空调、视频监控；

1.1.7 机房的搬迁、整合和系统的迁移；

详细清单见附件 1。

1.2 中心机房关键设备备件服务

服务期内，关键设备发生故障需要提供备件时，乙方应在第二个工作日（或 6 小时）内，将完好备件运抵现场，并派工程师在现场完成备件更换。备件范围包括附件内的所有设备。

1.3 设备维修及更换

若采购维保服务的设备发生故障时，乙方根据故障等级在第一时间到达现场并进行设备维修。如果设备维修后仍然无法正常使用，乙方须对设备进行更换，所更换设备必须为相同厂家不低于原设备档次的全新设备。更换设备所需费用由成交方承担。

2. 对第二行政区一号楼信息化相关设备设施运维

主要内容为对第二行政区一号楼提供网络(含 wlan)、大厅各办事

窗口标识屏（led 小屏）、各功能室大屏（d1p、lcd、pdp 拼接大屏等）灯光音响系统、音视频监控系统、UPS（包含配套电池）、引导大厅电脑电视等设备设施运行维护服务，安排专人负责相关设备设施的日常巡检和故障处理。提供不少于 20T 安全存储空间和多功能应急电源。

3. 对年度行政服务中心电子政务设备更新计划和方案编制

合同期内，成交方根据相关文件要求，每年 8 月中旬前要编制出下年度针对行政服务中心电子政务设备的更新（或新增）计划和方案。

（二）电子政务运维服务原则

1. 高可用性

通过中心数据机房设备运维，可以更高地提高系统的可用性，使用户获得更高的故障解决率，使系统停机时间更短；另外，通过定期巡检等预防性运维工作，可以大大减少故障的发生概率。

2. 节约成本

由于提供本地化服务，以及采取了更加有效的成本控制策略，因此，所提供中心数据机房高端设备运维服务的价格将更加具有竞争力，使用户在得到更加快速的备件服务、更加快速的故障响应以及更加贴近的 IT 服务的情况下，减少机房的运营成本。

3. 更高的服务质量

乙方提供基于 ITIL 的、符合业界最佳实践和工业标准的服务管理体系，建立了具有丰富企业管理和 IT 技术背景的工程队伍，能够为机房运维提供切实可行的管理和服务方案，包括建立计算机系统

设备档案、系统运维记录、系统运维记录和系统管理分析报告等服务项目，保障机房 IT 系统正常运行，提供更高质量的 IT 服务。

4. 集中精力关注主营业务

网络系统运维服务，使甲方解除系统宕机和发生故障的后顾之忧，极大降低人员成本、提高工作效率。在保证信息化系统的高效运行的基础上，借助信息化系统集中精力拓展自己的核心业务。

5. 专业化的梯队支持

乙方应组建专业化的梯队，解决电子政务运维中的各种技术问题：硬件、软件、局域网、互联网、数据库以及各种集成系统等，提供如系统运维、系统优化等全面的技术服务。并结合实际业务发展需求，提供相应的项目咨询和建议。

（三）运维要求

1. 制定完备服务方案

根据电子政务中心机房、电子政务网络、二区一号楼网络和电子显示屏系统、视频监控系统、灯光音响系统等实际情况，分析现有系统的业务特点和设备运行情况，提供完整的系统服务方案，包括设备巡检计划、维护保养时间计划表、虚拟化服务器系统提出整理整合迁移优化方案、存储空间规划整理优化方案、存储数据迁移方案、电子政务网络及线路地址规划和优化方案、数据库空间规划整理优化方案、各种设备预防性维护保养规程等。提供详尽的技术手册，实施严格的项目管理，成立专门的服务团队，指派项目经理作为甲方维保项目负责人，对服务支持实施严格的服务管理，统筹相关工作，以保证

报修服务正常高效运行。服务团队人员变动须经甲方同意。

2. 电子政务网络、机房、信息系统的运行监控

乙方对电子政务网络、信息系统、机房及动力环境等的运行时刻监控，以防为主，对运行监控中出现的问题（非正常事件）及时处理并如实向主管部门报告，确保政务网络及信息系统的正常、流畅、稳定运行。因监控不完善、处理不及时而出现的事件或事故后果，乙方承担全部责任。

3. 电子政务中心机房向政务云计算中心搬迁及系统迁移方案

机房设施搬迁时，乙方需制定完成搬迁实施方案，在实施方案中，要尽可能考虑全面，搬迁流程安排合理。方案中要明确保证各种硬件设备完好，保证数据的安全性和完整性；要求所有数据进行备份，发生意外时数据可进行恢复；要求有配件清单，设备发生损坏时可随时更换备件；要求所有相关操作均应有记录存档。方案中体现迁移规划、步骤、存在困难、解决办法和应急措施。

4. 服务响应时间

4.1 驻场服务

发生故障，驻场人员需第一时间赶到现场。乙方因特殊原因需更换指定工程师，应及时通知甲方，在甲方同意后指定合格的接替人员。

4.2 故障报修热线服务

提供全年 7×24 不间断的电话服务支持，不限次，响应时间不超过 10 分钟。甲方在使用维保范围内硬件或软件如遇到问题，都随时可以从乙方得到电话支持与帮助。

4.3 远程问题诊断和支持服务

提供 7×24 远程协助支持，响应时间不超过 10 分钟。若故障不能通过热线支持解决，乙方可使用远程支持服务工具对服务范围内的设备进行远程诊断，或通过其它远程方式为解决问题提供帮助。

4.4 现场支持服务

对于现场人员不能解决，并且通过电话支持和远程支持都不能解决的软件故障，乙方应安排经验丰富的技术支持工程师赴现场分析故障原因，制定故障解决方案。现场技术支持完成后，技术支持人员需向甲方提交现场技术服务报告，甲方签字确认，双方各自存档；另外针对现场服务相关内容，乙方需对甲方进行过程解释和现场培训。如果乙方无法在规定时间内恢复系统运行，甲方有权另请第三方维修，所发生费用由乙方承担。

5. 备件更换服务要求

全年 7×24 小时范围内，若采购维保服务的设备发生故障需要提供备件时，乙方应在第二个工作日（或 6 小时），提供不低于故障核心设备性能的备用机运抵现场，并派工程师在规定时间内恢复乙方生产系统。

对于维保范围内设备已经停产，不能提供相关板件更换的，明确告知乙方，并提供相应的解决方案保证甲方硬件的正常更换。

对于本项目维护过程中涉及到的配件应满足如下要求：配件来源于正当渠道；规格、型号与故障件完全一致；交付采购人配件为新件；备件费用由乙方负担。

6. 设备部件调整服务

因工作及业务需要，在维护的系统上增加新的应用或进行数据库等软件的安装与调整等工作时，乙方须派经验丰富的工程师电话技术支持，必要时到现场支持，成交方对突发事件要积极主动及时解决与处理，确保系统及业务的正常运行。如设备需扩容或新增配件时，须派经验丰富的工程师电话技术支持，必要时到现场支持，扩容或新增配件费用由服务乙方负担。

7. 设备更换服务要求

7.1 若采购维保服务的设备需要更换时，甲方应在一周内将更换设备运抵现场，并派工程师在规定时间内恢复采购人生产系统。

7.2 对于本项目维护过程中涉及到的更换设备及配件应满足如下要求：

对于维保范围内设备已经停产，不能提供相关板件更换的，明确告知甲方，并提供相同厂家不低于原设备档次的全新设备；配件来源于正当渠道；规格、型号与故障件完全一致；交付采购人配件为新件；

8. 软件升级服务

8.1 对清单中所包含硬件或软件厂家有更新的固件或软件补丁，应结合采购人现有设备情况，通过分析，确定是否需要更新固件或升级软件。

8.2 对于本项目保修过程中涉及到的固件或软件补丁应满足如下要求：固件或软件补丁来源于正当渠道；升级固件或软件补丁费用由乙方负担。

9. 故障处理

9.1 故障级别分类

根据故障的严重程度，故障级别由高到低分为一级故障、二级故障、三级故障、四级故障，划分如下：

1 级：系统崩溃，影响整个或部分业务范围；

2 级：系统中断但影响范围较小、性能严重下降影响整个或部分业务范围、性能受损业务尚可运行但影响整个业务范围；

3 级：性能受损业务尚可运行，但影响的范围极小；

4 级：设备有问题但没有明显影响（影响范围较小）、技术咨询和支持等；

9.2 故障解决

若甲方设备系统发生故障，根据故障级别，乙方须提供驻场服务、电话支持服务、紧急远程支持服务和现场支持服务，主要服务内容包括：

9.2.1 若出现 1、2 级别故障，响应时间不超过 10 分钟，若 30 分钟内无法通过电话支持、远程解决故障时应甲方要求，乙方应立即安排技术工程师 3 小时内赶到现场，并成立后方专家小组配合进行故障处理，找出故障发生原因和解决方法。工程师到场后 2 小时内解决软件故障，若是硬件故障，则第二日（或 6 小时）备件到达后 2 小时内完成配件更换，解决故障。

9.2.2 若出现 3、4 级别故障，响应时间不超过 10 分钟，若无法通过电话支持或远程解决故障时，甲方和乙方约定时间，由甲方安排

工程师到场解决。

9.2.3 对于维护清单以外的硬件设备（如软件或其他厂商设备）故障造成的问题，乙方需给出合理的建议。

9.2.4 对未明确原因的问题，供应商应协助甲方进行排查。

10. 预防性健康检查服务

10.1 首次项目交接：乙方应与前期设备的维护服务商对本次维保设备的配置、运行状况进行一次交接，并对本次维保设备做一次全面的检查、并建立维保的配置文档。

10.2 健康检查计划：每三个月对所有设备进行1次巡检服务，针对业务的重要性，提供现场健康检查服务；每半年对维保范围内设备及系统进行性能调优。

10.3 巡检内容：乙方对维保范围内的设备进行全面检测，确认设备运行状态，检查系统错误记录，排除潜在隐患，以确保业务系统能正常稳定的运行。

10.4 协助用户建立数据备份，保存及恢复系统，提供技术保障并提供一般性故障排除的技术手册。

10.5 固件升级和补丁安装：巡检结束后，如硬件或软件厂家有更新的固件或软件补丁，应结合甲方现有设备情况，通过分析，确定是否需要更新固件或升级软件。

系统维护期内，乙方对所有设备进行性能数据采集和分析，并在巡检结束一周内将系统性能分析维护报告提交甲方，若系统性能没有达到最优，则提出相应的性能调优建议及方案。

11. 技术咨询服务

乙方须提供 7×8 小时数据库、操作系统及网络与安全等多方面的技术支持与咨询服务，并能主动与甲方进行技术交流，提高甲方的系统使用能力。

12. 辅助故障定位服务

应具有主机、网络、数据库、存储、中间件等多厂商多平台协作支持能力，当出现涉及多厂商的故障时，乙方能通过协调、配合相关软硬件厂商，共同对系统故障进行排查，为甲方提供辅助故障定位服务。

13. 服务文档

乙方须对保修设备建立详实的设备档案，并及时更新。乙方负责在项目实施过程中，须将项目实施过程文档及时交付甲方。

14. 培训服务

14.1 定期技术培训：乙方成交后，应及时了解用户的应用情况，并针对应用情况，定期组织技术培训。内容包括服务器系统、数据库、集群软件、存储等日常基本操作和维护管理培训，时间不低于 24 课时。

14.2 现场培训：在系统维护时提供现场的技术培训，包括硬件和软件的日常操作、简单的维护和错误处理等。

15. 其他服务

对涉及系统的所有软硬件系统升级、改造、迁移和整合等工作提供无偿的技术支持服务。

第二部分服务内容：电子政务信息系统安全检查服务

按照国家信息安全有关法规政策要求，对电子政务信息系统进行检查，掌握信息安全总体状况，发现存在的主要问题和薄弱环节，进一步健全信息安全管理制，完善信息安全技术措施，提高信息安全防护能力。

(一) 检查范围

运行于电子政务外网的各部门的信息系统，包括自行运行维护管理以及委托其他机构运行维护管理的办公系统、业务系统、网站系统等。检查的重点是本部门的重要业务系统和门户网站。

(二) 检查内容

1. 信息安全组织管理

- 1.1 组织制定并落实信息安全管理规章制度情况；
- 1.2 组织制定信息安全工作计划或工作方案情况；
- 1.3 组织开展信息安全教育培训和督促检查工作情况；
- 1.4 查验岗位信息安全和保密责任制落实，特别是重要岗位信息安全和保密协议签订情况；
- 1.5 外部人员访问机房等重要区域管理情况。

2. 信息安全防护管理

2.1 网络边界防护管理。查看系统总体网络架构、子系统分布、终端节点、区域划分及边界防护措施等，重点检查：a. 网络分区分域合理性；b. 安全防护设备策略配置有效性；c. 互联网接入情况，是否有访问互联网的安全控制措施，是否留存互联网访问日志并定期进行

分析。

2.2 信息系统安全管理。检查信息安全风险评估、等级保护等安全管理制度落实情况。

2.2.1 服务器安全防护。重点检查服务器上应用、服务、端口以及系统补丁等情况，是否关闭了不必要的应用，服务、端口；账户口令强度和更新情况；病毒木马防护情况，是否使用技术工具定期进行漏洞扫描、病毒木马检测。

2.2.2 网络设备防护。重点检查网络设备安全策略配置有效性；账号口令强度和更新情况；是否使用技术工具定期进行漏洞扫描。

2.2.3 信息安全设备部署及使用。重点检查防病毒、防火墙、入侵检测、安全审计等安全设备部署及使用情况，以及安全策略配置的有效性。

2.3 门户网站安全管理。以防攻击、防挂马、防篡改、防瘫痪、防窃密为目标，对门户网站安全防护情况进行全面检查：

a. 系统管理账户和口令，清理无关账户，防止出现空口令、弱口令和默认口令；

b. 服务器补丁更新情况，关闭不必要的端口，停止不必要的服务和应用，删除不必要的链接和插件；

c. 网站目录结构，删除临时文件，防止敏感信息泄露；

d. 信息发布审核制度建立及落实情况；

e. 是否使用技术工具定期进行漏洞扫描、木马检测。

3. 信息安全应急管理

3.1 应急预案。重点检查本部门信息安全应急预案制定、修订、备案及宣贯培训情况。

3.2 应急演练。重点检查信息安全应急演练情况；已开展演练的，查看演练文档、记录（包括演练计划、演练方案、演练记录、演练总结报告等）。

3.3 应急技术支援。重点检查是否明确了应急技术支援队伍。已明确的，检查其服务合同及安全保密协议签订情况，了解掌握应急技术支援队伍基本情况以及开展的技术支援活动。

3.4 灾难备份。重点检查重要数据和重要信息系统备份情况；对采用社会第三方灾难备份服务的，检查其服务合同及安全保密协议签订情况，了解掌握灾难备份服务设施运维安全管理情况。

3.5 信息安全事件应急处置。重点检查本年度发生的信息安全事件及处置情况；发生过重大信息安全事件的，检查是否进行了及时处置，是否按照要求上报和通报。

4. 信息安全教育培训

重点检查信息安全和保密形势教育及警示教育情况，领导干部和机关工作人员参加信息安全基本技能培训情况，信息安全管理和技术人员参加信息安全专业培训情况等。

5. 信息安全整改工作

针对上次检查发现问题的整改情况。重点检查：

- a. 制定的整改计划及采取的整改措施；
- b. 整改效果以及是否开展了进一步的信息安全风险评估；

c. 年度检查情况报告完成情况，报告是否完整准确、符合要求。

(三) 其他要求

1. 开展信息安全检测机构具有检测专业资质；

2. 拥有专业安全检测人员，无犯罪记录，并与机构签订安全保密协议；

3. 拥有与开展技术检测相适应的安全检测设备与检测工具；

4. 对接入的检测设备进行风险控制，周密制定检查工作应急预案，防止因技术检测引发信息安全事故，确保被检查信息系统的正常运行；

5. 每年检查两次，检查后出具针对被检单位的检查报告和整改建议以及济源全市整体检查报告。

6. 责任

6.1 保密责任。乙方须签订保密责任书，不得泄漏项目、网络、机房、系统等相关信息。

6.2 事故责任。乙方须签订事故责任书，如不按相关规定、招标要求或合同约定进行运维造成事故的，乙方要承担全部责任。合同期内如出现网络与信息安全问题或事故须乙方承担全部责任。

合同附件 2:

济源市行政服务中心电子政务运维与安全检查服务 采购项目运维设备清单

电子政务机房及电源机房软硬件设备清单				
一、重要业务系统、数据库及中间件				
序号	业务系统名称	数据库及中间件	数量	单位
1	热线云系统	oracle、sqlserver、Mysql 等, weblogic、Tomcat、 Apache 等	1	套
2	数字城管		1	套
3	网站云		1	套
4	政务办公系统		1	套
5	vmware vSphere 虚拟化软件		1	套
二、主机系统				
序号	品牌	型号	数量	单位
1	IBM	BLADE H 刀片服务器系统	2	台
2	浪潮	NF5220	7	台
3	浪潮	NF8560	4	台
4	浪潮	NF190D	6	台
5	浪潮	NF180	1	台
6	浪潮	NF280G2	3	台
7	浪潮	NF260	2	台
8	浪潮	AS500G3	1	台
9	浪潮	NF5225	2	台
10	浪潮	NF290D2	1	台
11	浪潮	NF360	1	台
12	浪潮	NF380G2	2	台
13	惠普	DL380G6	7	台
14	惠普	HJ6WP2X	1	台
15	惠普	DL380G7	1	台
16	惠普	CNG011S531	1	台

17	DELL	PowerEdge R710	3	台
18	DELL	PowerEdge 950	1	台
19	格尔	KOAL SSL-E2010	1	台
20	IBM	Xseries 236	2	台
21	格尔	KOAL SRQ15-G-10000	1	台
22	其他		18	台
总计			68	
三、存储系统				
序号	设备	型号	数量	单位
1	IBM	System Storage DS3524	2	套
2	IBM	System Storage DS3512	2	套
3	紫光	ULStor5020	2	套
4	总计		6	
四、网络设备				
序号	设备		数量	单位
1	交换机	华为 S3500	6	台
2	交换机	华为 S2000	4	台
3	交换机	华为 9306	4	台
4	交换机	华为 6506	1	台
5	路由器	华为 ne20	2	台
6	负载均衡	F5 BIG-IP 1600 series	1	台
7	负载均衡	信安世纪	1	台
8	其他交换机	中兴、华为等	10	台
五、安全设备				
序号	设备	品牌型号	数量	单位
1	防火墙		13	台
2	VPN		2	台
3	流控		1	台
4	网络回溯分析		1	台
5	上网行为管理		1	台
6	堡垒主机		1	台

7	入侵检测		3	台
8	入侵防御		2	台
9	审计		1	台
六、其他				
序号	设备	品牌	数量	单位
1	空调	艾默生	4	台
2	UPS(40k)	艾默生	2	套
3	Ups(20k)	艾默生	2	套
4	自动灭火系统	天津瑞普	2	套
5	KVM		10	台
6	显示器		8	台
7	监控		1	套