

海南省大数据安全体系建设项目
绩效自评报告

评价类型：☐实施过程评价 ☒完成结果评价

项目名称： 海南省大数据安全体系建设项目

项目单位： 海南省大数据管理局

主管部门： 海南省大数据管理局

评价时间： 2023 年 01 月 01 日至 2023 年 12 月 31 日

组织方式：☐财政部门 ☐主管部门 ☒项目单位

评价机构：☐中介机构 ☐专家组 ☒项目单位评价组

评价单位（盖章）：
上报时间：

海南省大数据安全体系建设项目 绩效自评报告

一、项目概况

（一）项目基本情况

立项情况：根据《海南省政务信息化项目建设管理办法》（琼府办〔2020〕38号）有关规定，2020年，海南省电子政务外网安全体系改造纳入2020年度政务信息化项目计划。2021年4月13日，省电子政务外网安全体系改造获得省大数据管理局对初步设计的审核。

2021年5月，海南省政务大数据安全保障体系建设软件开发及服务合同完成初步设计，2021年7月，海南省政务大数据安全保障体系建设软件开发及服务合同通过初设批复；2021年9月启动招标，2021年9月30日联通数字科技有限公司中标海南省政务大数据安全保障体系建设软件开发及服务合同。

实施主体：省大数据管理局作为本项目的实施单位，负责项目立项申报、财政资金申请及预算执行，负责制定相关管理制度、项目建设的验收工作

项目资金：海南省大数据安全体系建设项目A、B包初步设计的批复资金总额为2635.06万元人民币，均为省财政资金。截至2023年度12月份省财政下达预算资金总额为2504.11万

元，其中 A 包预算：1181.21 万元；B 包预算 1060.68 万元人民币万元。

主要内容：

（1）海南省电子政务外网安全体系改造（A 包）

1）、对政务外网安全体系进行升级改造，进一步提升政务外网网络安全防护能力，满足等保 2.0 三级防护的要求；

2）、采用平滑升级手段，在不影响现有业务访问的基础上，实现海南省人民政府门户网站群的双栈协议转换，转换后海南省人民政府的门户网站群全面支持互联网用户采用 IPv4 和 IPv6 两种协议栈进行访问。

3）、扩大态势感知的监测范围，对市县单位重要的政务业务系统和网络进行监测，通过更广范围的流量和事件收集，更加全面的展示全省党政外网的安全态势，更快的发现问题并及时通告相应的相关单位，保护海南省关键信息基础系统和网络的安全。

4）、本次项目主要对海南省电子政务外网网络安全相关硬件产品进行采购，硬件设备需满足三年服务，具体清单如下：

序号	名 称	单位	数量
一	海南省电子政务外网安全体系改造		
1	服务器对外发布区		
3.1	电子政务外互联网发布区接入 VPN	台	1
	电子政务外互联网发布区接入 VPN 授权	个	10000
3.2	堡垒机	台	1
	堡垒机授权	个	15000
3.3	漏洞扫描	个	1
	web 应用扫描功能模块	个	1
	基线配置核查功能模块	个	1
3.4	云负载安全防护平台	套	1
	云负载防护平台授权	个	7000
2	电子政务外网区		
2.1	电子政务外网区办公接入 VPN10	台	3
	电子政务外网区办公接入 VPN10 授权（3 台共计）	个	40000
2.2	电子政务外网区办公接入 VPN14	台	2
	电子政务外网区办公接入 VPN14 授权（2 台共计）	个	20000
2.3	电子政务外网区办公接入 VPN12（应用信创部署）	台	2
	电子政务外网区办公接入 VPN12 授权（2 台共计）	个	10000
2.4	网络回溯系统	台	1
2.5	堡垒机	台	1
	堡垒机授权	个	15000
2.6	漏洞扫描	台	1
	web 应用扫描功能模块	个	1
	基线配置核查功能模块	个	1
2.7	时间服务器	台	1
2.8	万兆安全隔离网闸	台	7
2.9	云负载安全防护平台	套	1
	云负载防护平台授权	个	7000
3	办公区		
3.1	上网行为管理服务器端	套	1
	上网行为管理终端安全软件授权	个	10000
4	政务网站群双栈协议转换		
4.1	双栈协议转换设备	台	3
5	网络安全态势感知市县采集节点		
5.1	流量采集探针设备	台	20

（2）海南省政务大数据安全保障体系建设软件开发及服务合同（B包）

1）、建设海南省政务云监管平台，支撑监管部门对政务云的整体情况的宏观把控，推动委办厅局将应用系统积极迁移上云，更有利于政务数据共享和大数据应用。

2）、建设可信计算免疫平台，在公共服务平台的服务器上部署可信计算免疫平台软件，以主动防御的方式防止了各种已知/未知病毒、木马的非法启动和注入，从源头上（云操作系统）阻止了各类恶意软件的发作和破坏，保障服务器的安全运行。

3）、建设大数据安全保障平台。为数据安全运营与监管提供技术平台的支撑，利用加密、脱敏、溯源等安全技术，针对数据全生命周期中风险，为政务数据资源提供保护手段，为数据安全运营与监管提供技术平台的支撑，防范敏感数据泄漏与滥用。

4）、建立海南省政务安全制度规范体系。按照国家、行业以及海南省关于网络和数据安全的要求，结合大数据管理局的实际情况，建立安全制度规范体系，涵盖网络、系统与数据安全的管理、防护和运营等方面，为日常的管理运营工作提供依据。

5）、实施政务大数据安全运营监管服务。建立统一的大数据安全运营监管中心，以数据安全运营监管为核心，同时覆盖可能影响数据安全的系统和网络的安全运营的内容，通过大数据安

全运营监管服务体系，降低大数据安全风险，保障政务数据安全合规。

（二）项目年度预算绩效目标和绩效指标设定情况

1. 产出指标:

- （1）项目软硬件系统维护完成率不低于 98%
- （2）系统维护方的运行维护响应时间不高于 30 分钟
- （3）海南省大数据公共服务平台重大数据安全事件解决率达到 95%

2. 社会效益指标:

- （1）纳入政务大数据安全保障平台的重要业务系统大于 3 个。

海南省电子政务外网安全体系改造（A 包）。海南省电子政务外网目前承担全省 120 多家党政机关单位近千个业务系统，用户数量到达 10 万以上。海南省电子政务外网于 2020 年进行全面升级改造，具备了目前电子政务网网络方面的支撑能力。本项目对电子政务外网具体加固安全设备达成预算绩效目标说明如下：

1）、终端安全接入 VPN 设备集群：电子政务外网终端用户达到 10 万以上，大部分终端用户通过 VPN 方式接入电子政务外网进行对政务网相关资源的访问。

2）、网络回溯分析设备：实现目标要求流量处理能力大于 20Gbps，硬盘大于 96TB。

3)、双栈协议转换设备:为了解决部署在电子政务外网互联网区政府网站 IPv6 访问时出现外部链接及部分二三级页面天窗现象。对海南省人民政府门户网站群及下属单位对外服务应用进行双栈协议转换,全面支持 IPv6,实现公众用户访问,同时快速解决 IPv4 向 IPv6 应用迁移中普遍存在的由于外链导致的内容缺失难题,完成国家及海南省大数据管理局对门户网站群 IPv6 的考核要求。经过统计调研汇总目前有 60 个业务系统需要全面完成需要完成双栈协议转换工作,每个双栈协议转换设备支撑 25 个以上;

4)、办公互联网设备老旧替换:办公互联网区安全设备老旧且性能不足,为更好提升办公区访问的安全稳定,本项目对目前办公区的上网行为管理设备进行替换,并增加终端安全软件 300 个;

5)、本项目在政务外网区和内网区各部署 1 套云负载安全防护平台,总共提供 10000 点的客户端授权,平台实现对终端的资产管理、风险管理、策略管理、报表监控等能力;实现对被保护终端的主机加固、安全防护、恶意代码查杀等能力。

本项目建设已完成达成绩效指标设定情况:

1、对政务外网安全体系进行升级改造,进一步提升政务外网网络安全防护能力,满足等保 2.0 三级防护的要求;

2、采用平滑升级手段,在不影响现有业务访问的基础上,实现海南省人民政府门户网站群的双栈协议转换,转换后海南省

人民政府的门户网站群全面支持互联网用户采用 IPv4 和 IPv6 两种协议栈进行访问。

3、扩大态势感知的监测范围，对市县单位重要的政务业务系统和网络进行监测，通过更广范围的流量和事件收集，更加全面的展示全省党政外网的安全态势，更快的发现问题并及时通告相应的相关单位，保护海南省关键信息基础系统和网络的安全。

（2）海南省政务大数据安全保障体系建设软件开发及服务合同（B包）

按照等保 2.0 网络安全等级保护三级的要求，构建涵盖物理安全、平台安全、网络安全、主机安全、数据安全、应用安全等技术能力的政务外网安全防护体系，提供基于大数据场景的安全防御体系，保障政务大数据安全；同时加强网络安全管理体系和网络安全监管体系建设。实现全时、全域、全维的安全保障能力，为加快推进“智慧海南”建设，大力推动 5G 覆盖和应用，加强区块链、云计算、大数据、物联网等新型数字基础设施建设提供网络安全基础，推动信息化产业和高新技术产业跨越式发展。

二、项目决策及资金使用管理情况

（一）项目决策情况（包括决策过程和结果）

1. 2020 年，海南省大数据推进领导小组办公室同意将该项目纳入 2021 年度政务信息化项目计划。

2. 本项目于 2021 年 4 月 13 日获得省大数据管理局对初步设

计的审核。

3. 2021 年 8 月 X 日，“局长办公”会议同意我局 2021 年政务信息化建设项目经费使用计划。根据《海南省大数据管理局信息化项目管理暂行规定》。

2023 年海南省政务大数据安全保障体系建设软件开发及服务合同处于试运行阶段，组织专家团队进行试运行问题识别及风险分析，存在如下问题：

2023 年 4 月经过海南省政务大数据安全保障体系建设软件开发及服务合同会议决定得出项目制度风险，建设方组织架构的变更及国家制度的发布直接影响制度的适用性和普适性，存在项目质量风险。

2023 年 9 月经过决策分析，制定根据国家最新法律法规及建设方组织架构变更制度的方案完成编制。该决策不会增加成本，并降低后续制度修订的风险。

2023 年 9 月经过专家会议讨论，提出海南省政务大数据安全保障体系建设软件开发及服务合同风险，终验后的运营合同条款存在服务失控及资金流失风险。经过团队讨论与高层会议后决策签署补充协议，追加项目运营服务质保金，避免项目质量风险。

（二）项目资金（包括财政资金、自筹资金等）安排落实、总投入等情况

1. 海南省电子政务外网安全体系改造（A 包），批复资金为 2635.06 万元，均为省财政资金。2023 年 12 月份省财政下达年

初预算资金为 2504.11 万元，节约 130.95 万元，实际可执行预算资金为 2504.11 万元，执行率为 95%。

2. 海南省政务大数据安全保障体系建设软件开发及服务合同（B 包），2023 年不涉及项目资金落实、投入。

（三）项目资金（主要是指财政资金）实际使用情况

1. 海南省电子政务外网安全体系改造（A 包），2023 年支付中国电信集团系统集成有限责任公司（现更名为中电信数智科技有限公司）承建项目的合同费用共计 11,339,800.00 元。

2. 海南省政务大数据安全保障体系建设软件开发及服务合同（B 包），2023 年不涉及项目资金使用。

（四）项目资金管理情况（包括管理制度、办法的制订及执行情况）

1. 海南省电子政务外网安全体系改造（A 包），严格按照局内部的管理制度开展项目的各项活动。严格落实项目资金的专款专用，严格执行省大数据管理局的资金管理、费用支出等制度，严格执行会计核算规范。当前资金管理情况正常，支出依据合规，不存在虚列项目支出的情况，不存在截留、挤占、挪用项目资金情况，不存在超标准开支情况。

2. 海南省政务大数据安全保障体系建设软件开发及服务合同（B 包），制定了一套全面的资金管理制度和办法，以确保项目资金的合理、高效使用。建立了详细的资金申请和审批流程，

明确了不同级别和金额的审批权限，确保资金使用的透明性和合规性。

三、项目组织实施情况

(一) 项目组织情况（包括项目招投标情况、调整情况、完成验收等）

1. 海南省电子政务外网安全体系改造（A包），海南省电子政务外网安全体系改造于2021年09月24日通过公开招标，确定中国电信集团系统集成有限责任公司为中标单位，服务周期为12个月，当前系统投产运行（已竣工），服务期内发生调整情况如下：

（1）将天融信网络流量分析系统（V3 TopNTA TN-91808）变更为科来网络回溯分析系统 RAS6000SX，造价不变。

（2）将天融信协议转换交付系统（V3TopApp PCD-82218）变更为睿哲 IPv6 应用互通平台-6ATE，造价不变。

2. 海南省政务大数据安全保障体系建设软件开发及服务合同（B包），2021年5月完成初步设计，2021年7月通过初设批复；2021年9月启动招标，2021年9月30日联通数字科技有限公司中标，中标金额10606800元。

(二) 项目管理情况（包括项目管理制度建设、日常检查监督等情况）

1. 海南省电子政务外网安全体系改造（A包），为做好综合运维项目管理工作，确保各个业务系统的安全性、可用性、可靠

性、响应性、满意度和可保障性均满足业务要求，除执行日常巡检、监控、日报、周报制外，还建立了运维变更管理、事件管理、介质管理、账号管理等运维管理制度。并组织各项目承建方编写应急处置预案，通过定期组织演练验证应急预案的可执行性，同时提升各个项目运维团队的应急处置能力

2. 海南省政务大数据安全保障体系建设软件开发及服务合同（B包）

（1）责任体系管理

1) 政务信息资源共享开放责任制度、规定、方案等相关材料，明确第一责任人是本单位主要负责人

2) 明确本单位负责政务信息资源共享开放的责任部门、责任岗位、责任人等

3) 有政务信息资源使用审批制度、规定、方案等相关材料，实质上建立审批制度

（2）体制机制管理

1) 有政务信息资源使用审批制度、规定、方案等相关材料，实质上建立审批制度

四、项目绩效情况

（一）项目绩效目标完成情况。

1. 项目的经济性分析：

（1）海南省电子政务外网安全体系改造（A包）

在电子政务外网现有网络安全基础上进行改造，进一步加强电子政务外网安全防护能力，通过建设终端安全防护平台和可信计算免疫平台等，对服务器、办公电脑、手机等终端进行安全加固，保障设备安全运行。项目的经济效益主要是间接经济效益，能有效提升安全防护能力，降低政务数据运行风险，同时有效节约建设和运维经费，实现显著的经济效益，有助于节约型政府的建设。

（2）海南省政务大数据安全保障体系建设软件开发及服务合同（B包）

1）. 主要经济效益

一是避免重复建设，节约财政投资。本次建设海南省大数据安全体系项目，在电子政务外网现有网络安全基础上进行改造，进一步加强电子政务外网安全防护能力，通过建设终端安全防护平台和可信计算免疫平台等，对服务器、办公电脑、手机等终端进行安全加固，保障设备安全运行。项目的经济效益主要是间接经济效益，能有效提升安全防护能力，降低政务数据运行风险，同时有效节约建设和运维经费，实现显著的经济效益，有助于节约型政府的建设。通过建设统一的政府云监管平台，避免了省市及各个部门重复建设云监管平台、重复购买服务器硬件设备和系统软件、重复开发接口程序，并且避免由此造成的接口复杂、管理困难、维护成本高等问题。面向监管部门和委办局提供监管服务，消除对云平台的安全顾虑，增强政务用户对云平台的信任和

信心，促进政务业务广泛迁移上云，从而促进海南省政务云整个生态圈的良性发展。

二是降低数据安全风险，提升数据资源使用效益。保障政务数据互联互通，促进政务数据共享开放。通过本项目可以降低数据被窃取、泄露、篡改、滥用等多方面风险，形成标准统一、流程清晰、责任明确的政务数据安全工作机制，使数据安全保障能力明显提升。可以支撑政务大数据平台目前的数据资源服务体系的运行，在推进政务数据资源共享开放，推动利用数据资源进行增值开发利用等方面提供安全保障。

三是安全保障体系的集约优化，节约成本，提升保障效率。电子政务网络安全事关国家网络与信息安全，通过集中建设关键信息基础设施网络安全、数据安全建设和安全保障体系，能够减少安全隐患，有效地加强网络与信息安全保障能力，通过集约化建设节省了建设成本，实现安全保障能力共享，提升安全保障效率。

2) . 主要社会效益

一是集约优化，提高网络与信息安全保障能力。电子政务网络事关国家网络与信息安全，通过推进关键信息基础设施网络安全、数据安全建设和安全保障体系，能够减少安全隐患，有效地加强网络与信息安全保障能力。

二是对政策的响应和落实。海南省大数据安全体系建设是对《促进大数据发展行动纲要》（国发〔2015〕50号）、《中华

《中华人民共和国国民经济和社会发展第十三个五年规划纲要》（国发〔2016〕43号）、《大数据产业发展规划（2016-2020）》（〔2016〕412号）等国家文件的积极响应和落实，也是对《关于加强全省电子政务建设的实施意见》、《海南省加快推进“互联网+政务服务”工作方案》、《海南省促进大数据发展实施方案》中关于数据安全保障要求的贯彻执行，紧紧围绕海南省“数字政府”改革建设需要，结合“数字政府”建设情况，加快推进政务数据资源整合和共享，夯实大数据安全基础设施，增强数据安全保障能力，支撑网络空间健康发展，健全大数据安全发展组织体系，健全大数据发展制度标准体系、健全大数据安全防护体系，健全大数据安全运营保障体系，健全大数据安全应急保障体系。

三是保障政务数据互联互通，推进政务数据共享。随着政务数据资源开放共享水平显著提高，智慧政府建设取得阶段性成果。通过建立大数据安全保障平台，逐步建立海南省大数据安全保障体系，同时配套逐步健全安全管理制度、规范和标准，可以降低数据被窃取、泄露、篡改、破坏的多方面风险，使数据安全保障能力明显提升。形成标准统一、流程清晰、责任明确的政务信息采集、维护、共享工作机制。支撑政务大数据平台运行的高弹性、高可用、高安全、按需服务的资源服务体系的建成，在推进政务数据资源向社会开放利用，推动社会主体利用开放数据资源进行增值开发利用，促进信息消费和信息服务产业转型发展等方面提供安全保障。

四是保护政府公信力和形象。政务数据内容覆盖范围大，敏感程度高，一旦发生数据泄漏事件，就会对社会公众和政府部门乃至国家产生严重危害。建立完善大数据安全体系，有效防止政务数据安全风险，保护政务信息不受侵害，维护政府公信力和形象。

五是增强数据安全效益。为省大数据管理局提供先进的、科学的技术手段和管理依据，使大数据安全保障工作更加突出重点、统一规范、科学合理。可以大大降低重要数据及公民个人信息的泄漏风险，更好地遵循技术防范和管理并重的原则，提高整体管理水平和管理效益。

2. 项目的效率性分析:

(1) 海南省电子政务外网安全体系改造 (A 包)

电子政务网络安全事关国家网络与信息安全，通过集中建设关键信息基础设施网络安全、数据安全建设和安全保障体系，能够减少安全隐患，有效地加强网络与信息安全保障能力，通过集约化建设节省了建设成本，实现安全保障能力共享，提升安全保障效率。

(2) 海南省政务大数据安全保障体系建设软件开发及服务合同 (B 包)

1) 政务大数据安全保障平台通过海南省大数据安全体系建设项目 B 包建于 2021 年。

2) 政务大数据安全保障平台可对外提供数据脱敏、溯源、安全网关、接口审计等能力，通过采集主机、数据库、堡垒机、VPN、文件服务等日志，挖掘数据采集-存储-传输-使用-共享等数据全生命周期的潜在风险，并对数据资产进行梳理和防护，利用数据安全智能识别引擎及可视化技术，监控数据访问过程，对数据共享交换进行敏感数据识别和合规性检测，最终通过态势感知大屏实现数据流转与风险的可视化。

3) 政务大数据安全保障平台目前已接入 30 个核心系统，8 台采集探针覆盖电子政务外网与互联网两大区域，已实现接入系统的主机、数据库操作指令审计，对 VPN、堡垒机等日志进行实时解析，监测运维操作的数据安全风险；并通过定制化能力与业务深度耦合，完成共享交换平台 7687 个对外 API 的审计、开放平台的数据脱敏监管、大数据公共服务平台的数据库运维阻断等能力，配合数据安全运营服务，已输出较强的数据安全防护成果。

4) 编制海南省政务安全制度规范

按照国家、行业以及海南省关于网络和数据安全的要求，结合大数据管理局的实际组织架构情况，建立了完善的安全标准和管理规范，已发布数据安全相关规范 7 个：《数据安全管理办法》、《大数据管理局数据安全管理办法》、《大数据平台安全基线配置规范、标准》、《海南省政务数据分类分级指南》、《海南省大数据管理局政务网络与数据安全事件应急预案》、《海南省电子政务外网网络与数据安全应急响应管理办法》、《海南省电子

政务外网信息系统安全基线标准》。已形成安全制度规范体系，涵盖网络、系统与数据安全、防护和运营等方面，形成标准统一、流程清晰、责任明确的政务数据安全工作机制，为安全运营工作提供了有力依据，解决了仅依靠项目组人员的自身能力和意识开展工作弊端。

5) 实施政务大数据安全运营监管服务

数据安全运营服务参考国际领先 IPDR 体系，借助政务大数据安全保障一体化平台的技术支撑，从数据安全风险识别、风险分析、安全防护、响应处置制定数据安全相关审计模型 100 余个，形成数据全生命周期安全运行监管，覆盖可能影响数据安全的系统和网络的安全运营的内容，通过大数据安全运营监管服务体系，降低大数据安全风险，保障政务数据安全合规。

当前，安全运营团队已开展数据权限安全监管、数据输出安全监管、数据安全风险监测(7*24 小时)、系统安全检测、安全应急及重保服务、资产梳理等工作，依托于平台的告警与接口审计能力，填补了以往无技术手段进行数据安全风险监测的空白，可及时发现和解决潜在的安全威胁，提高政务云数据和网络的安全性。

自安全运营开展以来，依托政务大数据安全保障平台的能力，月均发现 400 余起风险告警，组织相关厅局单位进行闭环，并逐步将线下闭环流程搬到海政通。

3. 项目的有效性分析:

电子政务网络事关国家网络与信息安全，通过推进关键信息基础设施网络安全、数据安全建设和安全保障体系，能够减少安全隐患，有效地加强网络与信息安全保障能力。

4. 项目的可持续性分析：

（1）海南省电子政务外网安全体系改造（A包）， 为省大数据管理局提供先进的、科学的技术手段和管理依据，使大数据安全建设保障工作更加突出重点、统一规范、科学合理。可以大大降低重要数据及公民个人信息的泄漏风险，更好地遵循技术防范和管理并重的原则，提高整体管理水平和管理效益。

（2）海南省政务大数据安全保障体系建设软件开发及服务合同（B包）， 在本次数据安全项目的可持续性分析中，主要专注于项目如何长期维护数据的完整性、可用性和机密性，同时促进核心数据的合规性和道德标准。从技术层面，评估了数据加密技术和分类分级、脱敏的实施情况，确保它们能够适应不断变化的威胁。通过定期的安全审计检测这些措施的有效性，并根据评估结果调整安全策略。在组织层面，主要分析了数据安全培训计划的覆盖率和影响力，确保每位运维人员都能理解并实践我局数据保护政策。

（二）项目绩效目标未完成情况及原因分析

无

五、其他需要说明的问题

（一）后续工作计划

做好各业务系统的维护工作，确保整体业务系统安全性、可用性、可靠性、响应性、满意度和业务连续性均满足业务要求，除执行日常巡检、监控、日报、周报制外，还建立了各业务系统的变更管理、事件管理、介质管理、账号管理等维护管理制度。并组织各业务系统的承建方编写应急处置预案，通过定期组织演练验证应急预案的可执行性，同时提升运维团队的应急处置能力。有利于促进政府间业务的协同，提高政府行政效率，有利于提高政府管理水平。有利于促进业务协同，提高行政效率，确保政府部门的业务正常运行，有助于实现协同办公。有利于加强监管，提高管理水平，集约化的信息系统运行维护可有效节约财政资金。

（二）主要经验及做法、存在问题和建议

按照等保 2.0 网络安全等级保护三级的要求，构建涵盖物理安全、平台安全、网络安全、主机安全、数据安全、应用安全等技术能力的政务外网安全防护体系，提供基于大数据场景的安全防御体系，保障政务大数据安全；同时加强网络安全管理体系和网络安全监管体系建设。实现全时、全域、全维的安全保障能力，为加快推进“智慧海南”建设，大力推动 5G 覆盖和应用，加强区块链、云计算、大数据、物联网等新型数字基础设施建设提供网络安全基础，推动信息化产业和高新技术产业跨越式发展。

海南省电子政务外网目前承担全省 120 多家党政机关单位

近千个业务系统，用户数量到达 10 万以上。海南省电子政务外网于 2020 年进行全面升级改造，具备了目前电子政务网网络方面的支撑能力。目前电子政务外网安全设备还是沿用以前老旧设备，电子政务外网安全解决问题如下：

1、安全设备数量不足，无法支撑大规模用户及不同业务类型用户的使用。

2、安全设备性能不足导致出现流量瓶颈导致电子政务外网使用出现卡顿，目前网闸映射策略的开通未进行严格审核，开通后的策略也未进行有效的管理，这就导致业务系统的公网访问策略越开越大，直接暴露在互联网侧的业务资产越来越多，违规互联的安全风险无法得到收敛。

3、安全设备老旧，设备稳定的降低，容易导致因设备原因引起的网络故障，降低电子政务外网的可用性。

4、安全设备缺口导致出现安全问题时无法溯源追踪解决。

目前在互联网侧（政务外网对外发布区），缺乏流量监测设备，对于来自互联网侧的攻击流量，无法实现完整的监测；对于已构成安全威胁的攻击行为，无法实现完整的攻击溯源。同时，我们也缺乏针对互联网侧的站点健康监测，无法实现对互联网侧资产的攻击面评估。

在内网侧（政务外网侧），未实现对边缘系统的监测全覆盖。未覆盖的边缘系统分为两部分，一是我局四楼机房的部分部署于物理机的业务系统；二是各云厂商未向我局同步报备的业务系

统。以上两部分边缘系统，是省政务外网安全监测体系的盲区，被迂回攻击的安全风险较高。

5、安全设备的安全策略无法细化安全细粒度，导致电子政务外网整体安全度降低。

目前我省政务外网各个区域的防火墙和 WAF 设备，普遍未做多层防御体系设计。重要业务与普通业务的防御水位持平，导致防护策略只能宽松化，否则将影响业务运行。我们迫切需要构建起多层防御体系，区分重要业务与普通业务，设置不同的防御水位，根据实际业务需要进行适度且必要的安全防护。

6、重要节点安全设备没有备份，也会降低政务网整体安全体系的风险系数。

7、目前我省政务外网部署于各云的业务系统，存在大量的跨云互通行为，跨云互通网路策略的开通也未进行严格的审核。跨云互通将大大拓展攻击者的攻击范围，攻击范围的拓展意味着攻击者将更容易获得攻击跳板，同时更容易隐匿攻击路径，这些都将几何级放大内网网络安全风险。我们需要收紧跨云互通网路策略的开通，严格审核此类策略的必要性，并对其安全性进行评估。

基于上述问题，经本项目建设，增加相应的安全设备，在网络安全基础设施层面对电子政务外网进行安全加固，更好地完成项目目标。

电子政务网络事关国家网络与信息安全，通过推进关键信息

基础设施网络安全、数据安全建设和安全保障体系，能够减少安全隐患，有效地加强网络与信息安全保障能力。