清远市政务服务数据管理局

清政数函〔2022〕47号

B类

清远市政务服务数据管理局关于第20220266号提案答复的函

尊敬的蔡筱倩委员：

您提出的关于集中开展政务信息系统等级保护工作，提升网络安全防护水平的建议（第20220266号）收悉。经研究，现将提案办理意见答复如下：

首先，感谢您对我市政务信息网络安全工作的关心和支持。随着信息化的发展和普及，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，网络安全形势日趋严峻。我局一直以来重视网络安全及信息系统等级保护工作落实。

一、主要工作举措

（一）加强组织领导，健全工作机制

持续统筹好“数字政府”网络安全和系统平台建设工作，对标省开展的“数字政府”网络安全指数有关评估指标，针对我市存在的短板，切实摸清家底，实现纵深防御，加强监测预警，健全应急机制，制定整改方案，建立完善政务外网网络安全管理制度。成立以市主要领导为组长的网络安全工作领导小组，完善我市体制机制建设，制定《清远市电子政务外网安全体系建设总体方案》《清远市电子政务外网网络安全指引》《清远市电子政务外网网络安全管理规范》《清远市电子政务外网网络安全管理办法》《广东省大数据中心清远节点政务数据安全管理办法》《清远市政务数据分类分级指引》等一系列网络安全管理制度。

（二）网络数据安全工作的基本情况

1、加强网络数据安全建设。针对政务外网建立了一套安全防范体系，部署了防火墙、入侵检测、APT 以及综合日志管理等安全设备，及时监测政务外网运转情况，限制疑似中毒或有攻击行为的 IP 访问。此外还针对清远市门户网站等重要系统部署了 WEB 防火墙和业务审计，重点保护重要系统的安全和数据共享平台的稳定安全运行。为进一步加强政务云平台节点安全检测和防护能力，2021 年政务云平台增加了互联网区天幕边界防护设备、政务外网区御界高级威胁检测设备、管理区云安全资

源池、一体化安全运营平台建设。不断提升安全防范能力。通过省级网络安全罩、政务外网互联网出口 APT 监测、威胁情报分析等方式提升政务外网边界安全监测能力，建立数据全生命周期安全防护和窃密泄密监管机制。积极规划建设密码保障系统，开展密码应用安全性评估，逐步提高省政务云平台及业务系统的密码防护水平。建设智能终端接入安全管理平台，加强信息系统上线前风险评估，强化网络安全审计，确保省政务云平台和政务大数据中心安全合规运行。完善应急响应机制，加强应急响应演练，持续优化网络安全应急响应能力。2022 年 7 月，广东省“数字政府”政务云省市一体化安全运营平台清远节点网络流量总体平稳，成功拦截 1577372 次攻击，封禁 2799 起恶意攻击。拦截针对清远市政府门户和集约化平台网站的 444368 次攻击，未对业务稳定运行造成重大影响。清远市政务云应用系统网络安全监测发现并处理 11 个恶意后门事件。

2、加强网络数据安全保护。一是加快推进信息安全等级保护工作。根据《关于开展第二级以上网络系统定级备案和测评工作的通知》要求以及《中华人民共和国网络安全法》《信息安全等级保护管理办法》等法律法规规定和上级有关指导意见，我局自有 7 个二级以上信息系统 2022 年 5 月已经完成系统备案工作，备案后已经落实第三方测评机构对系统进行测评，测评工作仍在进行中，之后可出具符合要求的测评报告。**二是**定期

对政务云以及政务外网上的单位系统开展网络安全检查。安全运营人员每天对安全设备进行巡检，检查设备状态和安全告警事件；检查存在弱口令的主机，及时向业主方提出该风险存在，并要求及时整改；定期检查存在高危漏洞的主机，通过微信群聊向业主反馈，并要求尽快完成漏洞修复；定期对安全设备的系统版本、规则库和病毒库进行更新，保持安全设备良好的防护状态；每月通过省市一体化MSP安全运营平台向政务云平台用户发出安全风险告知函，并要求尽快完整漏洞修复。目前政务云上业务系统防护情况如下：政务云主机数量为1217台，天眼云镜agent共安装1217台，覆盖率达到100%；政务云业务系统（面向互联网出口）数量为107个，纳入WAF防护业务系统107个，防护覆盖率达到100%。重要网站监控共发现网站黑链31个，已告知31个，整改率为100%。**三是**加强政务信息系统的数据资产梳理，定期开展数据安全风险评估，全面深入探查数据安全底数。1、依托省市一体化的数字政府政务云安全体系能力，构建清远市数字政府政务云商用密码安全池。所有迁移上云的信息化系统均需做安全等保密评，确保信息安全。省市一体化政务大数据清远节点各子系统均部署在政务云的云资源上，不提供互联网访问使用，第三方安全机构会定期的进行安全扫描，运维团队定期修复漏洞。2、参考省相关标准规范，明确市公共数据分类分级标准规范，推动各单位、各区县开展公

共数据分类分级工作，治理后及时同步至市公共数据资源目录。以共享为原则，以不共享为例外，设立共享属性转换的机制和规则，要求定期对不共享数据进行排查并根据时下政策更新不予共享说明。3、参考省相关标准，明确市公共数据各级应对措施及达标标准，梳理可供交易的政务公共数据，推进数据要素市场化，鼓励数据开放与利用。提升监测维度能力，强化安全监督监管体系，构建“全市一盘棋”机制。构建公共数据流动监测体系，识别公共数据各环节流动情况，加强重要数据的安全管理，杜绝敏感数据泄露。4、开展高级威胁防护、态势感知、监测预警等日常数据安全运营，完善网络安全监测、通报预警、应急响应与处置机制，提升网络安全态势感知、事件分析及快速恢复能力，建立协同联动的网络安全运营监管能力和实战化的网络安全防控运营能力，建立技术平台提升安全监管的效率与能力，推进网络数据安全监管工作整体智治。5、加强日常数据运营人员安全意识培训及日常安全操作规范，避免人为数据安全事件。6、在系统角色设置上按最小权限设计和分配，没有设置超级管理员，将权限分散管理。如用户的政务数据编目挂接和用数权限必须经过申请，由对应层级的省/市/县区的管理员审核通过后才具备。截止 2022 年 8 月底，本市已提申请上云并发放资源的系统数为 253 个；其中具备上线运行的系统 106 个，上线安全评估提测系统 74 个，未申请测评系统 32 个，提

测率为 70%；已通过上线安全测评系统 40 个，测评通过率54%。

3、推进政务数据安全有序开放。

加强政务数据安全开放，完善政务数据数据开放共享标准。本市共发布上线数据目录 2211 个；按共享类型划分，有条件共享的目录数为 916 个，无条件共享的目录数为 1295 个；按数据类型划分，系统库表类的目录数为 167 个，服务接口类的目录数为 62 个，电子地图类的目录数为 23 个，文件类的目录为1959 个。总共有 223 个单位发起 523 个用数申请单、累计审计3330 个数据；总共有 15 个单位完成 106 个供数审核单、240 个数据的审核。

二、下一步推进网络安全及信息系统等级保护工作措施

根据您提出的建议，结合我市工作实际，今后将进一步加强以下几点工作:

（一）加强数据分类分级。加强政务信息系统的数据资产梳理，加快推进信息安全等级保护工作。明确资产状态。根据国家政策法规梳理当前数据的合规要求。为后续风险评估，分级管控提供基础。

（二）加强数据安全风险评估。定期开展政务数据安全风险评估，全面深入探查政务数据安全底数。评估当前数字政府与法律法规之间的差距，识别数据处理活动中的安全风险和脆弱性；评估现有的防护措施有效性。

（三）加强数据安全体系建设。根据清远实际，加快制定《政务信息资源管理办法》，规范政务数据安全管理；进行数据安全技术防护能力建设；组织数据安全教育培训。

（四）加强数据安全运营。对数据安全风险持续监测；进行数据安全事件应急响应；监测数据安全告警分析与组织汇报等工作。开展高级威胁防护、态势感知、监测预警等日常数据安全运营，完善网络安全监测、通报预警、应急响应与处置机制，提升网络安全态势感知、事件分析及快速恢复能力。

（五）为加强政务信息系统和电子政务外网的网络安全管理，增强单位干部职工的信息网络安全意识，提高信息安全自我保护能力，开展以信息安全意识的重要性、当前的信息安全形势、以及口令安全、环境安全、邮件安全等为主题的网络安全培训活动。

清远市政务服务数据管理局

2022年9月28日

（联系人：王蔚，联系电话：13802896349）

主题词：网络安全 政务信息系统等级保护

抄送：市政协提案委、市政府督查室