附件1-1

财政项目支出绩效目标申报表（项目总体情况）

（ 2019 年）

填报单位（盖章）　　金额单位：元

项目名称	区教育系统网络安全监管平台建设				
项目类别	一次性项目□　经常性项目■　中期预算试点项目□				
项目负责人：	张中涛	联系人：	王易	联系电话：	18917395678
起始日期：	2019-01-01		结束日期：	2019-12-31	
项目概况	闵行区教育局信息中心作为闵行区教育局职能科室之一。主要工作职责是制定全区教育信息化发展规划、工作计划等重要工作议案，落实推进教育信息化发展的重大事项；规划和部署全区教育信息化基础设施建设、教育管理信息化建设、教育信息资源开发与共享、教育信息化应用评估及教育信息化试验项目推进等工作；指导、检查、评估各中小学、各直属单位教育信息化建设与应用。 建设目标：以信息安全“事前威胁可视可知、事中风险可管可控、事后追责可证可信。”为目标，基于成熟的安全软件产品集成，建成一套基于大数据技术的闵行教育系统网络安全监管平台，对区教育局及所辖各中小学、各直属单位教育信息提供统一的网络安全监管，实现区内教育信息系统、网站、移动应用等网络安全可视化、监测预警，并结合专业安全服务商，提供技术上的指导从而快速处置已发生的信息安全事件、处置可能存在的威胁，实现主动风险管控。 经过前期对大量相关技术和主流产品的研究学习，项目内容包括： （1）○选购网络安全可视化、漏洞扫描、安全监测、流量审计、日志审计等软件； （2）○对相关产品进行集成，实现网络安全状态的统一展现，构建全区教育信息化的安全评估和风险可视化能力，包括应用系统及其组件的可用、性能、威胁、风险、漏洞的监测、预警和处置技术指导能力。 项目建设周期：于2019年内完工。				
项目立项情况	依　据:随着“三通两平台”、“一师一优课”的深入推进，以“三全两高一大”作为发展目标，我区教育信息事业不断引入“互联网+”、大数据、新一代人工智能等先进技术，进入了一个飞速发展的阶段。新技术的应用、信息系统的不断扩展，信息设备的不断增长，给信息化管理工作带来了全新的挑战，近年来发生的海莲花、暗黑客栈、白象舞步、丰收行动等一系列针对我国的安全事件，预示着“建好”不等于“管好”、“用好”。安全入侵事件、违规操作、错误操作等，往往源自系统漏洞、代码缺陷，伴随着日志非法删除，无法溯源、难以追责。区内各级单位安全防护专业水平不一，在某些单位处，核心数据库遭受数周暴力破解而不自知；尽管遵循等级保护的相关要求，定期开展安全基线检查，也仅在测评前才开展，难以做到漏洞的实时监测；《网络安全法》提出了对日志管理的要求，要落实日志管理，就要将海量安全资产的日志进行汇集、解析提纯才能看得懂，这需要耗费大量安全专家的资源，而投入只能针对特定场景，成本非常高昂。遵循《上海市教育信息化“十三五”规划》“强化防御体系，提高网络空间安全保障能力”中，“加强对信息系统、网站、移动应用的监测和预警能力，全面开展信息技术安全评估，强化信息安全服务体系，开展安全管理和技术培训。”的要求，以本项目为试点，构建覆盖全区、未来覆盖全市的网络安全监管平台，为全市教育信息系统、网站、移动应用等提供从监测预警到妥善处置的一体化集约安全保障能力建设，探索出一条可行之路。 必要性:我区教育对外服务和信息发布的网站多达510个，其中大量服务器放置在学校，当系统变更时存在大量的安全风险和漏洞。拟建项目是对已有系统安全建设不足之处的补充，以及进一步的完善和优化。 （1）目前闵行教育信息系统缺乏统一的安全监管平台，各级单位的安全状态不清晰、不透明，无法高效掌握安全形势并开展后续统一指挥、有序应急的安全保障工作。 （2）目前闵行教育信息系统，尤其是各下级单位，缺乏网络日志保存六个月的机制和应用的有效途径和方法，不符合《网络安全法》的要求；如果不建立统一可共享的平台，由各单位自建，则成本高、质量参差不齐。 （3）目前互联网每周都有大量的安全漏洞爆出，但缺乏有效的安全公告机制以及时发现应对各类安全漏洞；完全依靠人力开展漏洞扫描或由各单位自主购买漏洞扫描工具，成本高、质量难以保障。 （4）目前各级管理部门对信息安全等级保护要求的落实越来越严格，措施越来越多，依靠目前测评前临时组织自查、整改不能符合要求，且完全依靠人工进行安全技术检查效率低、覆盖范围小，造成大量不必要的人力资源消耗。 （5）外部攻击通常是针对各单位对外提供服务的网站发起，而这些网站由于开发公司不同，开发水平有限，开发的时候往往关注网站功能而不关注安全性，尤其是很多下面网站开发单位都已经不存在了，因此，需要需要对目前对外开发的网站做全面的梳理，并实时进行安全监测，主动发现存在的问题和异常，以便于及早将安全事故消灭在萌芽状态。 （6）一直以来，闵行教育的信息安全都是出于被动救火的模式，哪里有事故就到哪里去处理。无法掌握全局、无法主动发现弱点，这种被动救火的模式就只能延续下去。通过本项目的建设，就是要构建一套可以将网络安全技术方方面面的威胁、漏洞、弱点统一监控起来、统一展示出来，从而掌控全局、主动出击，实现从“被动安全”向“主动防御”的能力提升，为我市教育系统网络安全监管能力提升，摸索出一套可行的方案。 介于上述存在的不足与问题，提出针对的建设与改造。 可行性:项目建设的闵行教育系统网络安全监管平台总体实现方式是通过对应用安全监测、网络安全日志审计和流量审计软硬件产品的深度集成，构建统一的网络安全综合数据库，将三个安全产品的数据统一采集、处理和智能分析，并通过可视化的方式进行展现，从而实现“事前威胁可视可知、事中风险可管可控、事后追责可证可信。”这一网络安全监管目标。 从政策维度，自网络安全法发布以来，合法合规运营“三通两平台”一直是市网信、市教委对我区教育局的严格要求。积极响应市网信办建立覆盖各行业网络安全全面监管体系的要求，市教委作为教育行业主管单位，在全市层面开展网络安全公共服务平台建设的基础上，对我区教育局下达了区级网络安全的一系列试点任务，其中网络安全可视化监管平台建设作为核心任务之一，不仅可以实现从区到区属单位、学校的一体化集约安全状态可视，从而全面掌握网络安全风险、威胁的管控入口，更可以通过平台建设为市教委提供行业网络安全风险、威胁可视化监管智能化的算法、自动化分析规则和日志审计模板等可共享可复用的知识数据，同时，以遵循市教委网络安全公共服务平台相同的技术架构，通过项目建设的基于大数据技术的安全综合数据平台，为各种网络安全成熟产品的深度集成、集中展现、多点联动累计经验，因此项目具备政策可行性。 从技术角度，项目涉及到WEB安全监测、信息系统可用性监控、安全管控、日志采集和分析、综合展示等多种产品，要深入分析产品功能和实际需求的符合程度，要确定各产品的技术架构基本一致，产品应当成熟并具有可集成接口，并通过技术支持实现对接。项目将通过三方面降低风险：首先，选择的产品应优先自主可控并具有完全知识产权；其次，选择产品功能符合度高的厂商提供集成实施服务；第三是通过产品厂商提供运营服务来确保项目成果可用、可持续发展，为未来实现全市一体化集约的教育系统网络安全监管奠定基础，因此项目具备技术可行性。 从管理维度，历经多年悉心建设，我局现已形成成熟的项目管理体系，确保从规划到立项、从设计到研发、从建设到实施、从上线到运营的项目全生命周期得到精细化管理，从成本、进度、质量三方面均能够确保项目的正常开展，因此项目具备管理可行性。				
项目资金	一、项目总预算：1180000				
	二、当年预算：	1180000			
	（一）财政拨款：	1180000			
	1.上级财政拨款：				
	2.本级财政安排：	1180000			
	3.下级财政配套：				
	(二)其他资金：				
项目相关资源投入和制度建设情况	作为市教委构建一体化集约的网络安全监管平台的试点，区教育局已经完成全区信息系统大检查工作，完善了关键信息资产管控水平；开展了中小学门户网站集群建设，推进了信息系统集约化建设；加强了网络安全防护措施，强化了技术防范能力。下一步，就是要通过网络安全监管平台的建设，落实行业全面安全监管，并为市教委构建一体化集约的网络安全监管平台摸索出一条可行之路。当前区教育局已经投入大量人力资源进行相关产品的考察、测试验证和技术预研工作，并已于6月初向市教委、区委进行了闵行区教育系统网络安全试点工作汇报。 历经多年悉心建设，我局现已形成成熟的项目管理体系，确保从规划到立项、从设计到研发、从建设到实施、从上线到运营的项目全生命周期得到精细化管理，从成本、进度、质量三方面均能够确保项目的正常开展。 另外，从项目本身的建设内容来看，项目成果是对《网络安全法》发布后，落实法律要求、合法合规运营的一大助力，不仅从区教育局的角度建立起可一体化集约复用的网络安全威胁管控可视化平台，更从技术手段上，结合先进的大数据、智能化、互联网技术，有效促进下级各单位安全法要求、等级保护要求、自身信息安全管理制度的落实。				
项目总目标	（1）建设目标 以信息安全“事前威胁可视可知、事中风险可管可控、事后追责可证可信。”为目标，基于成熟的安全软件产品集成，建成一套基于大数据技术的闵行教育系统网络安全监管平台，对区教育局及所辖各中小学、各直属单位教育信息提供统一的网络安全监管，实现区内教育信息系统、网站、移动应用等安全可视化、监测预警，并结合专业安全服务商，提供技术上的指导从而快速处置已发生的信息安全事件、处置可能存在的威胁。 经过前期对大量相关技术和主流产品的研究学习，项目内容包括： 1)○选购安全可视化、漏洞扫描、安全检查、日志管理等软件； 2)○对相关产品进行集成，实现安全状态的统一展现和指数评估，构建全区教育信息化的安全状态量化评估能力、风险可视化能力，包括应用系统及其组件的可用、性能、威胁、风险、漏洞的监测、预警和处置技术指导能力。 （2）业务功能目标 事前威胁可视可知。通过网络安全监管平台的建设，将我局及所辖各中小学、各直属单位所有教育信息系统和组件，包括：网站、网络设备、安全设备、数据库、中间件、服务器、虚拟化服务器的五类网络安全综合数据：内容数据、可用性数据、性能数据、技术配置数据和日志数据，进行统一采集、存储、分析、展现、预警，实现基于网络安全综合数据的安全状态可视化、可量化评估、可识别潜在的威胁、漏洞、弱点。 事中风险可管可控。通过网络安全监管平台的建设，针对网络安全综合数据，通过安全可视和评估、漏洞扫描、安全检查、日志管理等功能的集成，运用自动化技术，实现对运作风险的监控、事件的快速发现和定位辅助、处置的技术支持，将已发生的风险影响控制到最小。				
年　度绩效目标	1、网络安全状态可视可知：教育信息系统和组件网络安全综合数据可采集率不低于80%（含虚拟化主机，不含桌面设备）；提供不低于12次威胁情报及时共享；WEB应用内容数据篡改实时告警成功率>90%/月；统一网络安全状态可视化展示大屏各功能可正常交付。 2、智能日志审计：实现操作系统、中间件、安全设备的智能日志审计，智能覆盖率>80%（接入设备数/所有设备数）。 3、自动化漏洞扫描：实现基于CNNVD（中国国家漏洞库）的主机系统定期自动化漏洞扫描，扫描覆盖率>70%（接入单位数/所有单位数）。 4、自动化流量审计：实现基于旁路的流量审计，可还原TCP、HTTP、DNS、POP3、SMTP、IMAP等流量，解析流量行为，提供网络抓包功能，攻击预警数>90%/月（预警攻击次数/总体攻击次数）。 5、可信综合日志存储：实现基于多租户的综合日志存储权限隔离功能，满足《网络安全法》保留网络安全日志不少于六个月的要求，实现6个月生产日志保全、24个月安全日志备份。				
需要说明的其他问题	无				

填报单位负责人：张中涛　　填表人：王易　　填报日期：2018年10月

附件1-2

财政项目支出绩效目标申报表（绩效目标）

（2019 年）

项目名称： 区教育系统网络安全监管平台建设　　金额单位：元

项目构成	主体活动（作业、任务）和对应产出的详细描述	闵行教育系统网络安全监管平台总体实现方式是通过对应用安全监测、网络安全日志审计和流量审计软硬件产品的深度集成，构建统一的网络安全综合数据库，将三个安全产品的数据统一采集、处理和智能分析，并通过可视化的方式进行展现，从而实现“事前威胁可视可知、事中风险可管可控、事后追责可证可信。”这一网络安全监管目标。选择的软硬件产品应是完全自主可控的产品，以便于进行多个产品的深度集成和开发；本着集约化原则，数据平台应遵循大数据架构，支持TB级数据下的准实时检索和存储资源动态、弹性扩展以及高可用，采用Elasticsearch,分析检索基于分布式搜索引擎，底层基于Lucene，采用多shard的方式保证数据安全，并且提供自动resharding的功能；网络安全监管平台的开发应采用B/S架构，遵从现有应用系统技术体系，使用的开发语言应为java，中间件应为apache，WEB服务器应为tomcat，数据库应为Microsoft SQL Server或MySQL；系统参考ANNs人工神经网络模型，基于Fann2MQL工具，使用Scilab及R语言开发，自动执行器基于PUPPT开发。 （1）应用安全监测产品软件采购实施　（2）日志审计产品软件采购实施　（3）流量审计产品采购实施　（4）统一网络安全威胁可视化展现子系统开发　（5）安全监管子系统开发　（6）证据保全子系统开发　（7）数据安全传输子系统开发（8）数据解构提纯子系统开发　（9）告警信息处理子系统开发　（10）智能分析子系统开发			
	一级目标	二级目标	三级目标	目标值	备　注
绩效目标	产出目标	数量	教育信息系统和组件网络安全综合数据可采集率	（4）不低于80%（含虚拟化主机，不含桌面设备）	采集对象数/总对象数
			自动化漏洞扫描：实现基于CNNVD（中国国家漏洞库）的主机系统定期自动化漏洞扫描	扫描覆盖率>70%	扫描对象数/总对象数
			智能日志审计：实现操作系统、中间件、安全设备的智能日志审计	智能覆盖率>80%	接入设备数/所有设备数
		质量	自动化流量审计：实现基于旁路的流量审计，可还原TCP、HTTP、DNS、POP3、SMTP、IMAP等流量，解析流量行为，提供网络抓包功能	攻击预警数>90%/月	预警数/事件数
			可信综合日志存储：实现基于多租户的综合日志存储权限隔离功能，满足《网络安全法》保留网络安全日志不少于六个月的要求	实现6个月生产日志保全、24个月安全日志备份	全区无该项违规事件
		时效	网络安全状态可视可知	主动识别率>50%	可视化威胁主动识别次数/总体威胁次数
			威胁情报及时共享	24小时内通报率>80%	24小时内的安全情报通报数/总体情报数
			WEB应用内容数据篡改实时告警成功率	2小时内告警率>90%	篡改2小时内告警数/总告警数
	效果目标	社会效益	提高我区教育信息系统的整体安全性、稳定性、可靠性	被动发现的安全事件数<20%	被动发现的安全事件数/总体安全事件数
			符合《网络安全法》“保存网络日志不少于六个月”的要求	全区教育系统100%符合网络安全法要求	执法检查不合法通报数为零
	影响力目标	长效管理	为区教育信息中心提供专业的安全咨询服务，包括应急预案修订及演练，等级保护咨询服	=100.00%	考察应急预案及相关等保测试报告
		满意度	客户满意率	=90.00%	考察客户对本项目的满意比率

	项目名称	项目内容	项目明细	明细金额	单价	依据	数量	依据	备注
项目构成分解	区教育系统网络安全监管平台建设	区教育系统网络安全监管平台建设　硬件购买类	区教育系统网络安全监管平台建设 硬件采购 安全产品-安全产品-360-分析平台主节点引擎-4*GE管理电口，3*USB3.0接口，1*DB9 Console接口，冗余电源，600G SSD + 12*4TB SATA 存储硬盘。含15个月产品标准维保服务，自发货之日起开始计算。含一年威胁情报更新授权	400000	400000.00		1.00		年度项目
	区教育系统网络安全监管平台建设	区教育系统网络安全监管平台建设　产品软件购买类	区教育系统网络安全监管平台建设 产品软件采购 工具软件-三零卫士-应用安全监测及展示产品—安全可视化产品、可视化地理信息产品、可视化安全评分	180000	180000.00		1.00		年度项目
	区教育系统网络安全监管平台建设	区教育系统网络安全监管平台建设　产品软件购买类	区教育系统网络安全监管平台建设 产品软件采购 工具软件-三零卫士-日志审计分析产品--日志采集与安全传输引擎、日志可信存储与备份模块、日志智能分析引擎、日志审计与分析模块、高级分析模块、审计分析报告模块、基础应用平台、基础数据平台、日志采集引擎对象授权、原始日志数据自动解构适配、多安全产品数据集中存储适配、告警合并与过滤	500000	500000.00		1.00		年度项目
	区教育系统网络安全监管平台建设	区教育系统网络安全监管平台建设　硬件购买类	区教育系统网络安全监管平台建设 硬件采购 安全产品-安全产品-360-流量采集探针-2*GE流量监听电口，2*10GE流量监听光口，2*GE管理电口，3*USB3.0接口，1*DB9 Console接口，冗余电源，4TB SATA存储硬盘。含系统软件一套	100000	100000.00		1.00		年度项目
金额合计				1180000	----	----	——	——	——

附件1-3

项目支出绩效目标申报表(制度保障)
（2019年）

项目名称：区教育系统网络安全监管平台建设					
制度保障	文件名称	具体措施	保障阶段		
项目管理制度	《闵行教育信息中心安全管理手册》	《闵行教育信息中心安全管理手册》：区教育局层面测定的信息化安全项目管理制度、用以规范项目实施管理，各相关单位应遵守执行，主要内容有项目管理流程、运维方案等。	立项和计划阶段 √	实施阶段 √	收尾和完成阶段 √
预算管理制度	《闵行区教育系统预算编制与执行暂行规定》	预算编制流程、部门审批流程、预算申报流程、预算批复流程以及执行管理	立项和计划阶段 √	实施阶段 √	收尾和完成阶段 √
财务管理制度	《闵行区教育局专项资金管理暂行办法》	职能部门分工、资金拨付流程、资金审批流程、会计核算方式	立项和计划阶段 √	实施阶段 √	收尾和完成阶段 √