国家计算机病毒应急处理中心

项目支出绩效目标表

（2025年）

国家计算机病毒协同分析平台（一期）建设项目-2024中央绩效目标表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 341204国家计算机病毒应急处理中心 | | | | | | 单位：万元 |
| 项目名称 | 国家计算机病毒协同分析平台（一期）建设项目-2024中央 | | | | | |
| 预算规模及资金用途 | 预算数 | 433.00 | 其中：财政 资金 | 433.00 | 其他资金 |  |
| 采购项目设备 | | | | | |
| 绩效目标 | 1.本项目拟建设我国自主可控的国家计算机病毒协同分析平台，构建基于多引擎的计算机病毒检测、分析、采集、共享等体系，提升我国网络安全行业病毒检测、防范和处置能力，填补国内计算机病毒协同分析平台空白，切实提高我国对全球互联网网络安全威胁的感知能力和整体安全防护能力。 | | | | | |

| 一级指标 | 二级指标 | 三级指标 | 绩效指标描述 | 指标值 |
| --- | --- | --- | --- | --- |
| 产出指标 | 数量指标 | 采购设备数量 | 采购设备数量 | ≥15台 |
| 质量指标 | 设备验收合格率 | 设备验收合格率 | 100% |
| 时效指标 | 支持每秒查询次数 | 支持每秒查询次数 | ≥10000次 |
| 数量指标 | 支持分析引擎接入数量 | 支持分析引擎接入数量 | ≥30个 |
| 成本指标 | 设备采购成本 | 设备采购成本 | ≤433万元 |
| 效益指标 | 可持续影响指标 | 设备使用时间 | 设备使用时间 | ≥10年 |
| 效益指标 | 社会效益指标 | 增强我国网络安全防护能力 | 增强我国网络安全防护能力 | 通过集中化的恶意代码扫描和分析，提升整体安全防护能力。 |
| 满意度指标 | 服务对象满意度指标 | 系统使用人员对平台的满意度 | 系统使用人员对平台的满意度 | ≥90% |

国家计算机病毒协同分析平台（一期）建设项目（非财政拨款）绩效目标表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 341204国家计算机病毒应急处理中心 | | | | | | 单位：万元 |
| 项目名称 | 国家计算机病毒协同分析平台（一期）建设项目（非财政拨款） | | | | | |
| 预算规模及资金用途 | 预算数 | 883.00 | 其中：财政 资金 |  | 其他资金 | 883.00 |
| 购置项目专用设备及服务 | | | | | |
| 绩效目标 | 1.项目总体建设目标是建设我国自主可控的国家计算机病毒防治关键信息基础设施（“国家计算机病毒协同分析平台”），基于对国内可信网络安全企业、国际知名网络安全企业的恶意代码分析引擎及相关技术资源的有效集成，通过各个组成模块之间的协同运行，实现对海量网络未知样本的实时多引擎比对分析，构建基于多引擎的计算机病毒检测、分析、采集、共享等体系，打造以我国网络安全产业为核心的网络与数据安全创新生态，填补国内计算机病毒协同分析平台空白，切实提高我国对全球互联网网络安全威胁的感知能力和整体安全防护能力。 | | | | | |

| 一级指标 | 二级指标 | 三级指标 | 绩效指标描述 | 指标值 |
| --- | --- | --- | --- | --- |
| 产出指标 | 数量指标 | 集成国内外主流引擎数量 | 集成国内外主流引擎数量 | ≥30个 |
| 数量指标 | 日均运行时间 | 日均运行时间 | 24小时 |
| 数量指标 | 支持常态在线人数均值 | 支持常态在线人数均值 | ≥1000人 |
| 时效指标 | 日均检测能力 | 日均检测能力 | ≥500000次 |
| 时效指标 | 每秒查询能力 | 每秒查询能力 | ≥10000次 |
| 成本指标 | 项目预算 | 项目预算 | ≤883万元 |
| 质量指标 | 个人用户注册、上传样本文件功能 | 个人用户注册、上传样本文件功能 | 支持 |
| 质量指标 | 重要单位、企业用户批量上传样本文件，并生成规范化的威胁情报信息功能 | 重要单位、企业用户批量上传样本文件，并生成规范化的威胁情报信息功能 | 支持 |
| 效益指标 | 社会效益指标 | 推动构建威胁情报共享和联合研判分析网络，有效联合社会力量，形成国内安全研究人员和企业的强大资源库 | 推动构建威胁情报共享和联合研判分析网络，有效联合社会力量，形成国内安全研究人员和企业的强大资源库 | 作用显著 |
| 效益指标 | 社会效益指标 | 协助追溯恶意软件来源、行为和传播路径，从而增强涉网络攻击、涉失泄密等安全事件线索信息的发现能力 | 协助追溯恶意软件来源、行为和传播路径，从而增强涉网络攻击、涉失泄密等安全事件线索信息的发现能力 | 作用显著 |
| 效益指标 | 生态效益指标 | 数据安全创新生态建设 | 数据安全创新生态建设 | 作用显著 |
| 满意度指标 | 服务对象满意度指标 | 服务对象满意度 | 服务对象满意度 | ≥95% |
| 满意度指标 | 服务对象满意度指标 | 企业满意度 | 企业满意度 | ≥95% |