渭南市网络安全检查技术服务**需求**

**一、基本要求**

1、功能要求：本项目需分为远程技术检测、现场督导检查、机房威胁评估三种方式。远程技术检测需要对100余个互联网系统（含网站）进行互联网信息收集、手工渗透，发现安全问题，并按照单位要求编写技术检测报告。现场抽查需要对单位进行现场检查工作和检查数据分析及报告整理编写。对机房内网开展技术检测，发现安全问题，并现场提供技术指导，按照单位要求编写技术检测报告。

|  |  |  |
| --- | --- | --- |
| 序号 | 内容 | 用途 |
| 1 | 全市网络安全技术检测 | 针对我市党政机关互联网业务系统（含网站）进行技术平台检测。 |
| 前期信息收集统计、人工漏洞挖掘、漏洞分析。 |
| 汇总形成漏洞整改建议和检测结果报告。 |
| 2 | 机房内网安全监测 | 监测网络流量中病毒、木马、蠕虫、僵尸网络，缓冲区溢出攻击、DDOS、扫描探测、欺骗劫持、SQL注入、XSS、网站挂马、异常流量、隐蔽通道、AET逃逸攻击等。 |
| 3 | 现场检查 | 深入县区对部分内网系统进行专项技术抽查。 |
| 根据技术检测结果，对于问题严重的区县进行现场访谈。 |
| 配合网信办根据检测及访谈结果进行现场反馈，现场根据各单位实际情况进行技术指导。 |
| 4 | 协助整改验证 | 根据检查结果对存在问题单位的情况进行跟踪，验证整改结果及有效性，并将整改结果、进度报市委网信办。 |
| 5 | 应急保障 | 重要敏感时期加强对渭南市重要网站和系统的监测防护，建立应急值班制度，并派至少2名工程师现场7\*24小时驻守，及时稳妥应对处置突发网络安全事件。 |
| 6 | 编制报告 | 将网络安全自查、网络安全抽查结果进行分析汇总，编制检查结果报告，并按照市委网信办领导要求进行修改完善。 |