安政办字〔2012〕57号

各县、区人民政府，市政府有关工作部门:

为进一步加强网络信息安全保障工作，维护公众利益和国家安全，国务院办公厅《关于开展重点领域网络与信息安全检查行动的通知》(国办函〔2012〕102号)、省政府办公厅《关于开展重点领域网络与信息安全检查行动的通知》(陕政办发〔2012〕91号)分别对网络与信息安全检查工作进行了部署，省工信厅印发的《重点领域网络与信息安全检查行动检查指南》(陕工信发〔2012〕355号)对信息安全检查工作进行了具体安排。现就进一步做好我市重点领域网络与信息安全检查工作通知如下:

一、检查目的

通过开展重点领域网络与信息安全检查，全面掌握我市重要网络与信息系统基本情况，分析面临的安全威胁和风险，评估安

全防护水平，查找突出问题和薄弱环节，以有针对性地采取防范对策和改进措施，加强网络与信息系统安全管理、技术防护和人才队伍建设，促进安全防护能力和水平提升，预防和减少重大信息安全事件的发生，切实保障网络与信息安全。

二、检查范围

此次检查的范围包括政府信息系统、金融、能源、通信、交通、广播电视、医疗卫生、教育、水利、环境保护、有色、化工、装备制造等重点行业的网络与信息系统，以及供水供电供热等市政领域的网络与信息系统。对事关国家安全和社会稳定，对地区、部门或行业正常生产生活具有较大影响的重要网络与信息系统（含工业控制系统，下同）进行重点检查。

三、检查方式

此次检查按照“谁主管谁负责、谁运行谁负责”的原则，采取自查与抽查相结合、以自查为主的方式开展。

（一）自查。市信息化工作领导小组办公室（市工业和信息化局）负责指导督促各部门和有关重点行业开展自查；各县区政府结合实际统筹安排本县区重点领域网络与信息安全检查工作；市级各部门负责本部门信息系统安全自查工作；有关重点行业的自查工作由其行业主管或监管部门统一组织实施（重点行业信息安全主管或监管部门见下表）。

序号	重点行业或领域	信息安全主管（监管）部门	序号	重点行业或领域	信息安全主管（监管）部门
1	政府信息系统	市电子政务办	10	水利(含供水)	市水利局
2	金融	人行安康中心支行	11	环境保护	市环保局
3	能源	市发改委	12	民用核设施	

4	公路	市交通局	14	煤炭	
5	广播电视	市文广局	15	钢铁	
6	社会保障	市人社局	16	有色	
7	医疗卫生	市卫生局	17	化工	
8	教育	市教育局	18	装备制造	

各县区、各部门和有关重点行业要全面系统地检查所涉及网络与信息系统的安全情况，深入分析存在的隐患和问题，认真编写自查报告。自查报告内容主要包括：重要网络与信息系统基本情况，整体安全状况的基本判断，安全风险和威胁分析评估结果，发现的主要问题，薄弱环节及整改情况、加强网络信息安全工作的意见和建议等。

（二）抽查。在各县区、各部门和有关重点行业认真开展自查的基础上，市信息办（市工信局）会同市公安局、市国家安全局、市保密局、市委机要局、市电子政务办等部门组成联合检查组，采取安全技术检测、现场核查等方式，对重要网络与信息安全系统进行安全抽查，查找安全漏洞和隐患，评估安全防护能力，研究提出改进和加强安全保障的措施建议并及时反馈抽查县区、部门和单位。

（三）整改落实。各县区、各部门和有关单位对检查中发现的薄弱环节和问题，要及时采取有效措施加以整改，因条件不具备不能立即整改的要采取临时防范措施，确保网络与信息系统安全正常运行。

四、检查的重点内容

（一）信息安全基本情况。

1、网络与信息系统基本情况。系统特征，包括系统停止运行

后对主要业务的影响程度，系统遭受攻击破坏后对社会公众的影响程度等；系统构成，包括主要软硬件设备的类型、数量、生产商等；信息系统技术外包服务，包括服务类型、服务提供商、服务方式、安全保密协议等。

2、安全管理情况。信息安全责任制建立及落实情况，包括信息安全主管领导、信息安全管理机构、信息安全工作人员履职以及岗位责任、事故责任追究等；按照等级保护等国家信息安全有关政策和标准规范建立和落实日常管理制度情况，包括人员管理、资产管理、存储介质管理、运行维护管理、年度教育培训制度等；信息安全经费投入等情况。

3、技术防护情况。按照等级保护、密码防护等标准规范要求，建立健全技术防护体系的情况；网络边界安全防护措施，包括不同网络或信息系统之间安全隔离措施、接入互联网或内部网络的安全控制措施等；服务器、网络设备、安全设备安全策略配置情况，应用系统安全功能配置及有效性等；重要数据传输、存储的安全防护措施；根据密码防护的特殊要求，检查在用的密码技术、密码设备和密码服务情况。

4、应急处置及容灾备份情况。信息安全事件应急预案制定和修订情况，预案演练情况及相关人员对预案的熟悉程度；灾难备件与恢复措施建设情况，应急资源（技术支撑队伍、备机备件等）配备和建设情况。

（二）存在的问题和面临的风险。

1、当前安全管理和技术防护中的主要问题及薄弱环节，制约安全防护能力提高的主要因素（包括法律法规、政策制度、技术手段等方面）。

2、统计国外产品和服务在主要软硬件设备和信息技术外包服务中所占的比例，分析网络与信息系统对国外产品和服务的依赖程度。

3、根据安全检测发现的漏洞和隐患，分析网络与信息系统存在的安全风险，判断面临的安全威胁程度以及具备的安全防护能力，评估网络与信息系统的总体安全状况。

五、时间安排

8 月 14 日，市信息办《关于开展重点领域网络与信息安全检查的通知》（安信化办发〔2012〕5 号）对全市重点领域网络与信息安全检查工作进行了安排，部分县区、行业主管（监管）部门、单位高度重视网络与信息安全工作，认真进行了自查，并按时报送了自查报告，但仍有部分县区、行业主管（监管）部门、单位没有按要求对网络与信息安全检查工作进行落实，没有报送信息安全检查报告。没有开展网络与信息安全检查的县区、行业、单位要立即开展信息安全自查，形成书面报告，于 9 月 20 日前报送市信息办。

9 月 30 日前，市信息办会同相关部门组成联合检查组对各县区、各重点行业、各部门开展网络与信息安全检查情况进行抽查。市信息办提出全市重点领域网络与信息安全总结报告报市政府和省信息化领导小组办公室。

六、有关工作要求

（一）加强组织领导。各县区、各有关部门要高度重视此次检查工作，切实加强组织领导，精心部署，明确检查机构和检查人员，落实工作责任，保障工作经费，确保检查顺利实施并取得实效。市信息办对检查工作统一指导、协调和督促；市公安局、

市国家安全局、市保密局、市委机要局、市电子政务办等有关部门要加强沟通配合，按照职责分工做好相关工作。

（二）加强安全技术检测。此次检查要重视使用专业技术手段，组织专业技术力量通过互联网对被抽查的网络和信息系统进行外部检测，重点对病毒木马、信息篡改等安全问题以及安全漏洞和隐患等情况进行检查，检验安全防护措施的有效性以及系统防病毒、防篡改、防瘫痪、防攻击、防泄密等能力。

（三）加强安全风险控制。此次检查要严格执行相关工作纪律，周密制定应急预案，强化风险控制措施，确保被检查的网络与信息系统正常运行。需委托外部检测机构进行检测的，要对相关检测机构的安全可靠性及其技术能力、管理水平严格把关，明确检测机构和检测人员的安全责任。要严格按照有关保密规定和要求，切实加强保密管理。

安康市人民政府办公室

2012 年 9 月 12 日

抄送：市委有关工作部门，市人大常委会办公室，市政协办公室，
安康军分区。
市中级法院、市检察院。各新闻单位。
中、省驻安有关单位。

安康市人民政府办公室　　2012 年 9 月 12 日印发