工业和信息化部
国家质量监督检验检疫总局
中国人民银行
国务院国有资产监督管理委员会
国家保密局
国家认证认可监督管理委员会

文件

工信部联协〔2010〕394号

关于加强信息安全管理体系认证安全管理的通知

国务院各部委、各直属机构，各省、自治区、直辖市工业和信息化主管部门、质量技术监督局、国有资产监督管理部门、保密行政管理部门，各直属检验检疫局，人民银行上海总部、各分行、营业管理部、省会（首府）城市中心支行、副省级城市中心支行：

信息安全管理体系认证是依据相关信息安全管理标准（GB/T22080－2008/ISO/IEC 27001：2005等），对一个单位信

息安全管理状况进行评价的过程。开展信息安全管理体系认证，有利于各单位规范信息安全管理，有利于企业特别是服务外包企业开拓国际市场。但由于认证活动涉及被认证单位组织体系、业务流程、网络拓扑、关键信息设备配置、安全防护情况及薄弱环节等敏感信息，如果管理不到位，造成敏感信息泄露，将会使被认证单位面临信息安全风险，甚至危及国家经济安全和利益。为加强信息安全管理体系认证的安全管理，减少信息安全风险，现就有关事项通知如下：

一、各级政府机关和政府信息系统运行单位，不得利用社会第三方认证机构开展信息安全管理体系认证。为确保国家秘密安全，涉密信息系统建设使用单位不得申请信息安全管理体系认证。

二、各级工业和信息化主管部门要了解掌握同级政府部门信息技术外包服务情况，结合实际提出安全管理要求；指导督促为政府部门提供信息技术外包服务的机构加强信息安全管理。为政府部门提供信息技术外包服务的机构申请信息安全管理体系认证时，若其认证范围涉及政府信息，须经工业和信息化主管部门同意。

三、国家认证认可监督管理部门要针对信息安全管理体系认证的特点，进一步完善信息安全管理体系认证管理办法和相关标准，严格信息安全管理体系认证机构的市场准入管理，加强资质审查和日常监管，规范认证行为，依法严肃查处违法违规认证活动。

四、基础信息网络和重要信息系统主管部门及国有资产监督管理部门应加强对行业和国有企业的信息安全管理，对信息安全管理体系认证提出管理要求。通信、金融、铁路、民航、电力等基础信息网络和重要信息系统运营单位确需申请信息安全管理体系认证，应事先报行业主管或监管部门同意，其他涉及国计民生的国有企业确需申请信息安全管理体系认证，应事先报国有资产监督管理部门同意，涉及国家秘密的应报保密行政管理部门同

意。通过认证后，应加强信息安全风险评估，及时排查安全漏洞和安全隐患。

五、申请认证单位应选择国家认证认可监督管理部门批准从事信息安全管理体系认证的认证机构进行认证，并与认证机构签订安全和保密协议，严格信息安全和保密管理，要求认证机构切实履行不泄露、不扩散、不转让认证信息的义务，保证重要敏感信息不出境。

工业和信息化部　　国家质量监督检验检疫总局

中国人民银行　　国务院国有资产监督管理委员会

国家保密局　　国家认证认可监督管理委员会

二〇一〇年八月十二日

抄送：国务院办公厅。

工业和信息化部办公厅　　2010年8月17日印发