国家发展和改革委员会
中华人民共和国公安部 文件
国　家　保　密　局

发改高技[2008]2071 号

关于加强国家电子政务工程建设项目信息安全风险评估工作的通知

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各省、自治区、直辖市及计划单列市、新疆生产建设兵团发展改革委、公安厅、保密局：

为了贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号），加强基础信息网络和重要信息系统安全保障，按照《国家电子政务工程建设项目管理暂行办法》（国家发展和改革委员会令[2007]第 55 号）的有关规定，加强和规范国家电子政务工程建设项目信息安全风险评估工作，现就有关事项通知如下：

一、国家的电子政务网络、重点业务信息系统、基础信息库以

及相关支撑体系等国家电子政务工程建设项目(以下简称电子政务项目），应开展信息安全风险评估工作。

二、电子政务项目信息安全风险评估的主要内容包括：分析信息系统资产的重要程度，评估信息系统面临的安全威胁、存在的脆弱性、已有的安全措施和残余风险的影响等。

三、电子政务项目信息安全风险评估工作按照涉及国家秘密的信息系统(以下简称涉密信息系统）和非涉密信息系统两部分组织开展。

四、涉密信息系统的信息安全风险评估应按照《涉及国家秘密的信息系统分级保护管理办法》、《涉及国家秘密的信息系统审批管理规定》、《涉及国家秘密的信息系统分级保护测评指南》等国家有关保密规定和标准，进行系统测评并履行审批手续。

五、非涉密信息系统的信息安全风险评估应按照《信息安全等级保护管理办法》、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》和《信息安全风险评估规范》等有关要求，可委托同一专业测评机构完成等级测评和风险评估工作，并形成等级测评报告和风险评估报告。等级测评报告参照公安部门制订的格式编制，风险评估报告参考《国家电子政务工程建设项目非涉密信息系统信息安全风险评估报告格式》（见附件）编制。

六、电子政务项目涉密信息系统的信息安全风险评估，由国家保密局涉密信息系统安全保密测评中心承担。非涉密信息系统的信息安全风险评估，由国家信息技术安全研究中心、中国信息安全测

评中心、公安部信息安全等级保护评估中心等三家专业测评机构承担。

七、项目建设单位应在项目建设任务完成后试运行期间，组织开展该项目的信息安全风险评估工作，并形成相关文档，该文档应作为项目验收的重要内容。

八、项目建设单位向审批部门提出项目竣工验收申请时，应提交该项目信息安全风险评估相关文档。主要包括：《涉及国家秘密的信息系统使用许可证》和《涉及国家秘密的信息系统检测评估报告》，非涉密信息系统安全保护等级备案证明，以及相应的安全等级测评报告和信息安全风险评估报告等。

九、电子政务项目信息安全风险评估经费计入该项目总投资。

十、电子政务项目投入运行后，项目建设单位应定期开展信息安全风险评估，检验信息系统对安全环境变化的适应性及安全措施的有效性，保障信息系统的安全可靠。

十一、中央和地方共建电子政务项目中的地方建设部分信息安全风险评估工作参照本通知执行。

附件：《国家电子政务工程建设项目非涉密信息系统信息安全风险评估报告格式》

（此页无正文）

国家发展改革委　　公　安　部　　国 家 保 密 局

二○○八年八月六日

主题词：风险评估　　通知

抄送：中央办公厅、全国人民代表大会常务委员会办公厅、国务院办公厅、中国人民政治协商会议全国委员会办公厅、最高法院办公厅、最高检察院办公厅

附件：

国家电子政务工程建设项目非涉密信息系统信息安全风险评估报告格式

项 目 名 称：_____

项目建设单位：_____

风险评估单位：_____

年 月 日

目　　录

一、风险评估项目概述

1.1 工程项目概况

1.1.1 建设项目基本信息

工程项目名称		
工程项目批复的建设内容	非涉密信息系统部分的建设内容	
	相应的信息安全保护系统建设内容	
项目完成时间		
项目试运行时间		

1.1.2 建设单位基本信息

工程建设牵头部门

部门名称	
工程责任人	
通信地址	
联系电话	
电子邮件	

工程建设参与部门

部门名称	
工程责任人	
通信地址	
联系电话	
电子邮件	

如有多个参与部门，分别填写上

1.1.3 承建单位基本信息

如有多个承建单位，分别填写下表。

企业名称	
企业性质	是国内企业/还是国外企业
法人代表	
通信地址	
联系电话	
电子邮件	

1.2 风险评估实施单位基本情况

评估单位名称	
法人代表	
通信地址	
联系电话	
电子邮件	

二、风险评估活动概述

2.1 风险评估工作组织管理

描述本次风险评估工作的组织体系（含评估人员构成）、工作原则和采取的保密措施。

2.2 风险评估工作过程

工作阶段及具体工作内容.

2.3 依据的技术标准及相关法规文件

2.4 保障与限制条件

需要被评估单位提供的文档、工作条件和配合人员等必要条件，以及可能的限制条件。

三、评估对象

3.1 评估对象构成与定级

3.1.1 网络结构

文字描述网络构成情况、分区情况、主要功能等，提供网络拓扑图。

3.1.2 业务应用

文字描述评估对象所承载的业务，及其重要性。

3.1.3 子系统构成及定级

描述各子系统构成。根据安全等级保护定级备案结果，填写各子系统的安全保护等级定级情况表：

各子系统的定级情况表

序号	子系统名称	安全保护等级	其中业务信息安全等级	其中系统服务安全等级

3.2 评估对象等级保护措施

按照工程项目安全域划分和保护等级的定级情况，分别描述不同保护等级保护范围内的子系统各自所采取的安全保护措施，以及等级保护的测评结果。

根据需要，以下子目录按照子系统重复。

3.2.1 XX 子系统的等级保护措施

根据等级测评结果，XX 子系统的等级保护管理措施情况见附表一。

根据等级测评结果，XX 子系统的等级保护技术措施情况见附表二。

3.2.2 子系统 N 的等级保护措施

四、资产识别与分析

4.1 资产类型与赋值

4.1.1 资产类型

按照评估对象的构成，分类描述评估对象的资产构成。详细的资产分类与赋值，以附件形式附在评估报告后面，见附件 3《资产类型与赋值表》。

4.1.2 资产赋值

填写《资产赋值表》。

资产赋值表

序号	资产编号	资产名称	子系统	资产重要性

4.2 关键资产说明

在分析被评估系统的资产基础上，列出对评估单位十分重要的资产，作为风险评估的重点对象，并以清单形式列出如下：

关键资产列表

资产编号	子系统名称	应用	资产重要程度权重	其他说明

五、威胁识别与分析

对威胁来源（内部/外部；主观/不可抗力等）、威胁方式、发生的可能性，威胁主体的能力水平等进行列表分析。

5.1 威胁数据采集

5.2 威胁描述与分析

依据《威胁赋值表》，对资产进行威胁源和威胁行为分析。

5.2.1 威胁源分析

填写《威胁源分析表》。

5.2.2 威胁行为分析

填写《威胁行为分析表》。

5.2.3 威胁能量分析

5.3 威胁赋值

填写《威胁赋值表》。

六、脆弱性识别与分析

按照**检测对象、检测结果、脆弱性分析**分别描述以下各方面的脆弱性检测结果和结果分析。

6.1 常规脆弱性描述

6.1.1 管理脆弱性

6.1.2 网络脆弱性

6.1.3 系统脆弱性

6.1.4 应用脆弱性

6.1.5 数据处理和存储脆弱性

6.1.6 运行维护脆弱性

6.1.7 灾备与应急响应脆弱性

6.1.8 物理脆弱性

6.2 脆弱性专项检测

6.2.1 木马病毒专项检查

6.2.2 渗透与攻击性专项测试

6.2.3 关键设备安全性专项测试

6.2.4 设备采购和维保服务专项检测

6.2.5 其他专项检测

包括：电磁辐射、卫星通信、光缆通信等。

6.2.6 安全保护效果综合验证

6.3 脆弱性综合列表

填写《脆弱性分析赋值表》。

七、风险分析

7.1 关键资产的风险计算结果

填写《风险列表》

风险列表

资产编号	资产风险值	资产名称

7.2 关键资产的风险等级

7.2.1 风险等级列表

填写《风险等级表》

资产风险等级表

资产编号	资产风险值	资产名称	资产风险等级

7.2.2 风险等级统计

资产风险等级统计表

风险等级	资产数量	所占比例

7.2.3 基于脆弱性的风险排名

基于脆弱性的风险排名表

脆弱性	风险值	所占比例

7.2.4 风险结果分析

八、综合分析与评价

九、整改意见

附件 1：管理措施表

序号	层面/方面	安全控制/措施	落实	部分落实	没有落实	不适用
	安全管理制度	管理制度				
		制定和发布				
		评审和修订				
	安全管理机构	岗位设置				
		人员配备				
		授权和审批				
		沟通和合作				
		审核和检查				
	人员安全管理	人员录用				
		人员离岗				
		人员考核				
		安全意识教育和培训				
		外部人员访问管理				
	系统建设管理	系统定级				
		安全方案设计				
		产品采购				
		自行软件开发				
		外包软件开发				
		工程实施				
		测试验收				
		系统交付				
		系统备案				
		安全服务商选择				
	系统运维管理	环境管理				

序号	层面/方面	安全控制/措施	落实	部分落实	没有落实	不适用
		资产管理				
		介质管理				
		设备管理				
		监控管理和安全管理中心				
		网络安全管理				
		系统安全管理				
		恶意代码防范管理				
		密码管理				
		变更管理				
		备份与恢复管理				
		安全事件处置				
		应急预案管理				
小计						

附件 2：技术措施表

序号	层面/方面	安全控制/措施	落实	部分落实	没有落实	不适用
1		物理位置的选择				
		物理访问控制				
		防盗窃和防破坏				
		防雷击				
		防火				
	物理安全	防水和防潮				
		防静电				
		温湿度控制				
		电力供应				
		电磁防护				

	网络安全	网络结构安全				
		网络访问控制				
		网络安全审计				
		边界完整性检查				
		网络入侵防范				
		恶意代码防范				
		网络设备防护				
	主机安全	身份鉴别				
		访问控制				
		安全审计				
		剩余信息保护				
		入侵防范				
		恶意代码防范				
		资源控制				
	应用安全	身份鉴别				
		访问控制				
		安全审计				
		剩余信息保护				
		通信完整性				
		通信保密性				
		抗抵赖				
		软件容错				
		资源控制				
	数据安全及备份与恢复	数据完整性				
		数据保密性				
		备份和恢复				

附件 3：资产类型与赋值表

针对每一个系统或子系统，单独建表

类别	项目	子项	资产编号	资产名称	资产权重	赋值说明

附件 4：威胁赋值表

资产名称	编号	威胁																		总分值	威胁等级
		操作失误	滥用授权	行为抵赖	身份假冒	口令攻击	密码分析	漏洞利用	拒绝服务	恶意代码	窃取数据	物理破坏	社会工程	意外故障	通信中断	数据受损	电源中断	灾害	管理不到位	越权使用	

附件 5：脆弱性分析赋值表

编号	检测项	检测子项	脆弱性	作用对象	赋值	潜在影响	整改建议	标识
1	管理脆弱性检测	机构、制度、人员						V1
		安全策略						V2
		检测与响应脆弱性						V3
		日常维护						V4
		……						V5
2	网络脆弱性检测	网络拓扑及结构脆弱性						V6
		网络设备脆弱性						V7
		网络安全设备脆弱性						V8
		……						V9
3	系统脆弱性检测	操作系统脆弱性						V10
		数据库脆弱性						V11
		……						V12

4	应用脆弱性检测	网络服务脆弱性						V13
		……						V14
5	数据处理和存储脆弱性	数据处理						V15
		数据存储脆弱性						V16
		……						V17
6	运行维护脆弱性	安全事件管理						V18
		……						V19
7	灾备与应急响应脆弱性	数据备份						V20
		应急预案及演练						V21
		……						V22
8	物理脆弱性检测	环境脆弱性						V23
		设备脆弱性						V24
		存储介质脆弱性						V25
		……						V26
		……						V27

9	木马病毒检测	远程控制木马							V28
		恶意插件							V29
		……							V30
10	渗透与攻击性检测	现场渗透测试	办公区						V31
			生产区						V32
			服务区						V33
			跨地区						V34
		远程渗透测试							V35
11	关键设备安全性专项检测	关键设备一							V36
		关键设备二							V37
		……							V38
12	设备采购和维保服务	设备采购环节							V39
		维护环节							V40
		……							V41
13	其他检测	……							V42