

《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)

2003年9月7日中共中央办公厅、国务院办公厅发出通知，转发《国家信息化领导小组关于加强信息安全保障工作的意见》，并要求各地结合实际认真贯彻落实。

《国家信息化领导小组关于加强信息安全保障工作的意见》是为进一步提高信息安全保障工作的能力和水平，维护公众利益和国家安全，促进信息化建设健康发展而提出的。具体意见有以下几点：

- 一、加强信息安全保障工作的总体要求和主要原则
 - 二、实行信息安全等级保护
 - 三、加强以密码技术为基础的信息保护和网络信任体系建设
 - 四、建设和完善信息安全监控体系
 - 五、重视信息安全应急处理工作
 - 六、加强信息安全技术研究开发，推进信息安全产业发展
 - 七、加强信息安全法制建设和标准化建设
 - 八、加快信息安全人才培养，增强全民信息安全意识
 - 九、保证信息安全基金
 - 十、加强对信息安全保障工作的领导，建立健全信息安全管理责任制
- 省国家保密局对部分省级机关计算机信息系统进行保密检查

根据中共中央保密委员会办公室、国家保密局有关对计算机信息系统使用管理情况进行保密检查的通知要求，根据国家保密局和省国家保密局有关涉密计算机和上国际互联网计算机使用保密管理的规定、标准要求，省国家保密局在各地以及省直机关单位自查的基础上，于7—8月对部分省直机关单位计算机信息系统使用管理情况进行了抽查检查工作。从目前已抽查的部分省直机关单位重要部门、要害部位的保密检查中发现存在以下问题：

- 1、目前，我省大部分单位的内部局域网还没有经保密部门审批。省局多次发文，各单位内部办公局域网的保密问题仍没有引起足够重视。
- 2、按中办发〔2003〕17号文规定，电子政务网络划分为涉密网和非涉密网，即

电子政务内网和电子政务外网。有部分单位对网络的划分不明确，所有的网络接在 INTERNET 上。

3、有的部门的涉密计算机随意通过电话线就可上国际互联网；有的在自检自查后，还有部分计算机中有过上国际互联网的历史；少数部门还存在上国际互联网的计算机存储涉密信息的严重问题。

4、涉密计算机管理不严。在我们检查时办公室门开着，计算机开着，但人不在，计算机上存有各种内部信息。有的单位至今还没有制定涉密计算机、上国际互联网计算机相应管理制度的问题。普遍存在涉密计算机不设防，磁介质不标密，管理跟不上，监督检查不落实的状况。

5、涉密计算机系统建设、使用须按国家有关规定履行一定的验资和审批手续，才能进行建设和投入使用。但至今仍有少数部门在建涉密计算机系统时对国家有关规定置若罔闻。在招投标中对施工方不验涉密系统资质，网络系统安全保密方案不申报审批，建成的涉密网络不经审批就运行的情况时有发生。

涉密计算机上国际互联网和上国际互联网计算机涉及国家秘密问题，都是泄露国家秘密的行为，必须引起各级领导高度重视。希望各地、各部门、各单位针对以上问题认真进行检查，切实把计算机的安全保密问题提高到关系国家安全和利益，关系到电子政务安全、健康、有序地发展的高度来认识。并加强保密组织领导，加大宣传教育、督促检查的力度，增强各级领导和干部的保密意识，落实保密工作责任制，切实加强涉密计算机和上国际互联网计算机的使用和保密管理，做到既充分发挥计算机在推动办公自动化和信息化进程的积极作用，又确保国家秘密信息的安全。

电子政务安全保密的若干问题

一、电子政务与保密工作部门的关系？

保密工作部门在电子政务建设与应用中的职责是安全保密管理。安全保密管理是电子政务安全保密体系框架的安全保密要素之一。安全保密管理涉及方方面面，也涉及电子政务建设和应用的全过程。电子政务安全保密体系框架还包括其他安全保密要素：安全保密策略、安全保密法规、安全保密组织、安全保密标准、安全保密服务、安全保密技术和产品、安全保密基础设施。安全保密管理与各个

要素是密切相关的。管理要明确策略，比如“涉密最小化”就是一种策略，目的是保重点、保核心，做到该保的一定保住，该放的一定放开。管理还要健全法规，比如保密法的修改就要考虑电子政务及政务公开、信息公开等情况。用法律法规明确哪些政务、信息公开，哪些要保密，规范行为，保障电子政务建设和应用的健康发展。我们知道，管理是通过组织机构去实现的，电子政务建设中要健全有关安全保密组织。管理要完善标准和规范，比如政务内网就要按照涉密网的相关保密标准去要求，管理还要规范服务，加强系统安全保密测评和安全保密培训。另外，管理在安全保密技术与产品方面体现在推动技术进步和产品的检测认证方面。在安全保密基础设施建设中也要加强安全保密管理，比如公钥基础设施 PKI 和备份与灾难恢复系统的安全保密管理。

二、保密工作部门在电子政务中要做哪些工作？

总体来讲，保密工作部门在电子政务建设与应用中要做好安全保密管理工作。具体来讲，应体现在以下几个方面：

（一）正确界定涉密网络，做好政务内网和政务外网的划分。

政府部门在建设电子政务时，普遍遇到的问题是：对于本地区、本部门政务内网和政务外网的划分难于把握。即涉密网(政务内网)要不要建，要建多大才既有利于保密又方便工作。过去有一种误区，认为：网络划分是政务部门的事，只要你划为涉密网了，保密工作部门再按涉密网的要求去管理。这样的结果往往造成对上网的业务信息资源涉密程度界定不清，网络划分不够合理，造成先天不足，增加了安全保密管理的难度。保密工作部门在电子政务建设的规划阶段，应协助政务部门，结合实际需求，正确界定涉密网络，做好政务内网与政务外网的划分。

（二）重点抓好政务内网建设与应用中的安全保密管理。

政务内网是涉密网，就要按照中央保密委员会以及国家保密局的一整套对涉密网的要求去管理。保密工作部门对电子政务安全保密管理的重点就是抓好政务内网的安全保密管理。安全保密管理要贯穿政务内网建设与应用始终。

（1）督促政务部门对政务内网的安全保密设施要同步规划，同步建设。预留并保证安全保密建设经费。

（2）加强涉密信息系统集成资质单位的管理、监督和培训，要求政务部门选择具有涉密信息系统集成资质的单位承担政务内网的设计和建设。

(3) 积极向政务部门宣传涉密信息系统保密要求，使政务部门清楚具体要求，正确掌握标准。

(4) 协助政务部门抓好政务内网安全保密方案设计和论证，降低由于方案存在先天不足带来的安全保密风险。

(5) 加强工程监理，确保在政务内网实际工程建设中落实方案提出的各项安全保密措施。

(6) 做好系统测评，由国家保密局涉密信息系统安全保密测评中心及相关机构采用现场检测与专家评估的方式对政务类网进行测评，给出测评结论，作为审批的基础。

(7) 网络运行前检查和督促政务部门安全保密管理组织、人员和制度的落实，实施严格审批。

(8) 网络通过审批运行后，加强检查，发现问题及时堵塞漏洞，消除隐患。

(三) 加强政务外网和政务网站的保密管理

政务外网规模大，用户多且与互联网逻辑隔离，存在较大的安全风险。保密工作部门对于政务外网的保密管理主要体现在明确要求，督促检查，确保国家秘密信息不在政务外网上处理，确保政务外网与政务内网和其它涉密网络物理隔离。

政府网站包括中央政府及各部门和各级地方政府及各部门的网站，构建在互联网上。网站上发布的信息将会在全世界范围被知晓。保密工作部门对政府网站的保密管理主要体现在监督有关部门严格执行上网信息保密审查制度，严禁涉及国家秘密的信息上网。加强上网信息的保密检查，一经发现涉密信息，应立即删除，并严肃查处和追究有关人员的责任。