文章题目	美国政府对公共部门首席信息官电子政务的安全建议
发表日期	2006-6-13 13:24:23
内　　容	

来源：中国电子政务信息网

信息安全国家重点实验室

这是一份美国全国州首席信息官协会关于如何提高公共部门信息安全水平的建议书，它面向地方、州和联邦政府首席信息官这样一批特殊读者，以建议的形式发出一种行动呼吁。借鉴美国政府在此方面长期工作所形成的丰富经验和教训，对信息保障问题进行深入思考，对形成具体、可实施性强的中国信息安全保障国家战略或许会有所裨益。

电子政务会给社会公众和公司企业带来许多直接好处。与此同时，安全风险和脆弱性也在与日俱增。电子政务需要具有前瞻性的IT管理和稳固的基础设施。如我们所知，网络攻击、系统故障和自然灾害都会使整个体系运转不畅。如果我们的数字基础设施在关键部位出了问题，政府的运作就会陷于瘫痪，从而酿成灾难性后果。

建议一：建立一个相关人员都参与的IT管理结构

设计一个涉及所有风险承担者的IT管理结构，该结构应该包括企业级安全管理，应能在政策上做出应急反应，并适于通过检查实施领导的工作方式。

在美国，公共部门的IT管理安排分别采用了以下3种特点各不相同的模式中的一种。

大学模式

许多州对首席信息官的安排可以称作是“大学式”的。在这种安排中，首席信息官直接对州长负责，对首席信息官的任命来自州长和州内阁的决定。大学式管理看上去像一张网，其中以首席信息官(以及州长)为中心，影响力和指令由此向外辐射到各部门、委员会和利益集团。首席信息官通过长期计划、资金奖励、政策和人际关系进行管理。首席信息官的人员班子通常规模很小，但其中都是政治联盟的重要人物。

基于法规的安排

几乎有相同数量的州对IT管理采用基于法规的安排方式，这些州都有成熟的组织体系和法律。基于法规的结构通常设有一个执行理事会，通过审批总结、制定政策、标准和计划行使监督职能。这种安排下的首席信息官人员班子比大学式班子要庞大些。基于法规的首席信息官人员设计了汇报程序、计分卡和例外报告。这是一种等级分明的结构，它自上而下行使职责，通过各委员会提出重要方案。

基于角色的安排

如今，已有越来越多的州开始采用基于角色的安排方式。基于角色的模式通常都设有一个由各方代表组成的中央执行理事会，理事会的代表来自所有分支、教育机构、地方单位和私营部门，州首席信息技术设计师是支持理事会的后盾。理事会负责政策、长期计划、项目管理标准和企业IT管理体系方面的工作，企业安全也在理事会的监督之下。这种管理模式在设计上是模块化的。

IT管理绝不仅限于上述3种模式，地方、州和联邦政府往往会综合采用各种模式。就州一级政府而言，这种IT管理模式应该把政府的所有分支均涵盖在内，应该明确安全工作领导权并任命一个机构负责监督政策和指令的执行情况。政府的所有分支都应服从于企业整体体系及其共享基础设施、项目管理标准、安全表现度量标准以及用于外部和内部审查控制的审计标准。

IT安全还必须与州和地方政府级的应急反应相结合。由于州政府居于地方政府与联邦政府之间，因此会在这种结合中发挥主导作用。此外，州政府的这种地位还会因其IT基础设施与城市、镇区、县以及涉及公众生活和工作的其他管辖范围联系密切而得到强化。出于这一原因，州政府应该将其IT基础设施与地方和联邦政府的IT基础设施完全融合到一起。

建议二：实现企业安全计划目标

实现企业安全计划目标，其中包括对成功以及最佳处理方法做出评估，同时确保所有部门共享资源。

安全依赖于人及其专业水平和合作态度。在庞大的政府机构中，有许多IT技术人员和业务专家，他们掌握各种高新技术，对IT系统的建设起着重要作用。怎样协调涉及专业领域如此广泛的庞大员工队伍，对于首席信息官来说是一种严峻挑战，共享的IT基础设施和巨大的应用工作量使这种挑战进一步复杂化了。要想应对这样的局面，首席信息官必须寻求制定一整套前后连贯的设计原则和标准处理方法，并根据信息管理原则做出技术选择。

首席信息官的任务绝非仅仅牵涉技术和管理，而首席技术官的工作重心也超出了IT情况研究的范畴。中央IT基础设施开发官负责技术方面的工作，侧重于资源共享，而设计师的工作重点则是技术标准。一般而言，技术设计师最好不兼任首席信息官。这种职务的分离有利于监督和平衡。设计师通常负责规划和制定标准，而首席信息官则负责实施和管理技术体系和标准。这两个职务在规划功能上是重叠的。

建议三：开发安全度量标准

开发安全度量标准，以准确测定有害入侵、破坏安全和易受攻击环节。相关报告应以摘要形式分发给州政府的行政、立法和司法分支以及其他政府机构。报告应在政府单位中严格保密。

为了使安全这条主线贯穿机构的计划和文化，首席信息官需要开发一套报告标准，用以清晰显示安全要求是否得到满足。这套标准所依据的是以下几个重要信息来源。

审计结果

内部和外部审计员对总体控制和应用控制做出评价，决定需要采取什么级别的审计来确定财务报告的准确性和可靠性。审计工作可以找出管理方法以及安全方面的缺陷。对于首席信息官、IT基础设施开发官、首席安全官、首席技术官和首席技术设计师来说，负责评价与IT系统和安全相关的具体控制的审计员是一种内容丰富的信息来源。

入侵企图和渗透

IT安全官会对审计报告中出现的入侵次数以及渗透次数、渗透级别和渗透性质感兴趣，他们对来自内部和外部的攻击次数高度敏感。这方面的信息应该在企业的部门一级上收集，然后通过首席信息官上报给企业管理层并进入IT管理结构体系。

病毒报警和恢复

必须有一个常备中心、入侵反应小组或类似的部门清楚病毒何时渗入了本机构，它们是如何冲破安全网闯进应用中的资源的，以将受病毒侵害的系统恢复过来。分布式拒绝服务攻击、病毒、蠕虫、黑客、物理破坏和软件故障仅仅是这类问题中的几种。要点在于，首席信息官要知道这些事件的增加何时超过了底线。此外，首席信息官还必须了解是什么因素造成了出现峰值。

全国警报

对于首席信息官和首席安全官来说，全国警报是一大重要信息来源。有许多全国性组织发出全国警报并向用户提供预订服务。如计算机应急反应小组、全国基础设施保护中心、关键信息安全联盟、系统管理、网络技术和安全学会、全国州地理信息理事会、州际安全信息共享和分析中心等。

许多州建立了州际安全信息共享和分析中心，以帮助本部门安全官分析危险的入侵。这些州际安全信息共享和分析中心通常与一个常备中心相连，由这个中心协调州政府的应急反应和恢复工作。

有些州际安全信息共享和分析中心由机构内部成员组成，便于州首席安全官向本系统负责IT的官员发出警报。这些中心还便于成员共同就入侵事件进行分析和提出反应建议。随着州际安全信息共享和分析中心的发展逐渐成熟，它们还将配备硬件、软件、网络和物理安全方面的专家。它们还将拥有接受过紧急事件管理训练、精通IT灾难预防和恢复的应急反应专家。

建议四：配置安全技术

以下建议涵盖了组织机构用来选择适宜安全技术的各种方法。在下面的例子中，IT安全体系被划分为3个级别。至于应该选择哪个安全级来保护某一特定资产，则取决于该资产的重要性、脆弱性和价值。必须有一份最新并且准确的IT资产清单方能开始安全级选择程序。

第一级：基本级

这个最低级别是指最低限度安全体系。基本安全包括对物理进入数据中心和企业网络的控制，需要有持卡进入和日志报告之类验证程序才能物理进入数据中心和其他安全区。此外，需要有密码才能电子进入IT系统，密码至少应该有9个字符，由大小写字母、数字和符号组成。软件应能拒绝重复使用的或与个人使用的历史密码十分接近的密码改动，密码必须每隔两周或四周改动一次。最后，对于基本安全处理方法来说，网络扫描和病毒保护至关重要。

第二级：中级

中级安全要求体系强调进入IT系统者必须接受全面验证。验证范围包括公共关键基础设施、生物测定、密码卡技术或者可用来证实某使用者确实是提出申请者本人的变量。此外，复查技术也常常用来证实某些装置已得到授权进入网络。

就关键任务应用而言，管理员要对用于紧急调整的密码负责。这些密码保存在密封的信封里锁起来，每个只能使用一次，所有密码均由至少256位加密算法编写而成。最后，使用者在两次适当输入正确密码和/或用户名失败后将被禁止进入系统。所有例外都被记录在日志中，由系统管理员及系统拥有者独立进行检查。

密码卡技术可允许使用者每次执行任务均使用惟一的密码，这项技术通常用于执法用途，密码使用一定时间后就会注销。此外，密码是完全加密的，安全管理员会严密监督密码卡的使用。更为尖端的网络扫描、事务覆盖(如隧道技术)和请求回叫技术也可用在中级安全的安全系统上。最后，以这一安全级通过网络的关键数据应该完全加密。

第三级：高级

最高安全级由防御转入了进攻。网络能够了解什么人正在寻求进入某一特定系统，一旦出现非授权进入或非授权进入企图，就会发出警报。通过全面认证、基于应用安全的确认和全面授权可以掌握使用者的情况。

确保安全是一项代价高昂的艰巨工作。要想实施总体和应用控制，就必须满足以下3个标准。第一，首先必须建立控制体系。第二，控制体系必须有效运转。第三，对控制体系的运转必须通过独立的管理验证加以监督。这3个要求的任何一个没有被满足，严格意义上的控制就不可能存在。

建议五：开发州安全入口

前文讨论过的核心小组还应含有一个安全设计小组，以向管理常备中心和安全信息共享和分析中心(ISAC)人员提供帮助。除管理应急反应外，还负责管理供依赖州政府服务的机构、社会公众和公司企业使用的一个安全入口。该入口有一个安全且面向公众的登录网站，可协助应急管理人员发出通报，及时帮助处于危机中的公民。它还有助于协调企业对灾难和重大破坏事件的反应。

建议六：建立州际安全信息共享和分析中心

许多州缺乏人员和资金建立自己的州际安全信息共享和分析中心。各州政府意识到，这方面的服务需要很大开支，而寻找才智足以击退黑客攻击的人才也十分困难。应对黑客对基础设施的深层攻击这项工作需要很高的专业技能，以联邦部门ISAC模式建立的州际安全信息共享和分析中心可以在专业技能方面提供相关服务，同时将各州有关黑客攻击事件的数据收集到一起，用以支持网络安全国家战略规划的实施。

此外，州际安全信息共享和分析中心还可以帮助各州政府协调对网络攻击做出的反应，同时在执法部门和国防部门之间提供联络服务。协调工作的内容还包括传播有关审计的例外情况以及实施监督部门、内部审计员和联邦机构提出的安全标准的最佳处理方法。对于州内安全信息共享和分析中心，州际安全信息共享和分析中心必须承担有关通用审计和安全标准的人员培训工作。

建议七：提出样板式信息共享州立法法案

要想协调反应行动、了解关键基础设施的情况、制定全国战略和交流网络安全的最佳处理方法，各州政府就必须相互共享敏感的安全信息。然而，这方面的信息一旦落到居心不良者手里，就会变成贻害无穷的武器。州际信息共享一直很受限制，原因就在于各州政府担心，一旦本州信息出了本州州界或者交流给地方或联邦政府部门，本州的安全活动就会在其他州的公开记录中披露。此外，州首席信息官很

难协调某部门、理事会或委员会高度敏感的安全信息的交流活动。然而，协调信息共享对于保护关键基础设施来说至为关键。这就需要在州和联邦级别上分别立法，以确保安全报告在各级政府之间的交流在保密条件下进行，安全、隐私权和公开记录三者必须达到平衡。最后，立法应该禁止私营公司泄漏通过正常渠道从政府部门获得的敏感安全信息。

安全是一项艰巨的工作。只让安全官员、技术人员和IT执行人员来承受这副重担是完全错误的，确保安全是企业全体成员的共同职责。安全体系要建立在开放、资源共享和重点突出的文化基础上，绝不能只是在出现意外事件时才想起安全体系。要想使安全工作行之有效，各级政府就应该向全体雇员传授控制标准，同时把标准处理方法纳入计划和计量程序中。政府部门应该通过审计报告和度量结果提供反馈信息，以确定安全工作是否运转正常。

回到目录

上篇文章 美国电子政务考察报告 2006-6-13 13:44:02