文章题目	美国电子政府信息安全指标体系及其应用
发表日期	2006-7-5 8:38:52

内　　容

出处：计算机安全　日期：2006-7-1

在美国等西方发达国家的信息安全建设中，关键基础设施安全始终是重中之重。但是，由于绝大多数关键基础设施不由政府所控制，这些国家多次强调要使政府自身信息安全成为全国各部门、各行业信息安全的榜样，以次带动关键基础设施领域的信息安全工作。因此，大力发展电子政务，确保电子政府安全，已经成为西方发达国家政府日常运转中的重要任务。那么，“榜样”究竟表现如何？2006年3月16日，依据最新的电子政务信息安全指标体系，美国众议院政府改革委员会发布了2005财年联邦政府各部门信息安全评分结果。在24个被考察的政府部门中，正可谓“几家欢喜几家愁”。

1、电子政府信息安全评分制度的法律依据

以办公自动化为起点的电子政务开展以来，美国联邦政府就授权管理和预算办公室（OMB）负责开展与政府信息资源管理有关的工作，OMB也先后在此方面制定了多项规章制度。OMB所定义的信息资源包括了所有类型的信息以及由各种软、硬件构成的信息系统，信息安全是其中的重大问题，因此OMB在历史上逐渐成为美国电子政务信息安全的主要管理部门。2000年，美国颁布了《政府信息安全改革法案》（GISRA），以法律形式规定了政府各部门必须对其电子信息系统进行风险评估，并定期向OMB报告。

2002年，基于GISRA以来的经验，美国将GISRA更新为《联邦信息安全管理法案》（FISMA），并将其作为《电子政府法案》的第三章。FISMA正式确立了对联邦政府各部门的信息安全进行年度评估并向OMB报告的框架。根据这一法案，OMB报告的来源有两方面，一为联邦政府各部门的负责人，另一来源则为政府各部门内的总检查长（简称IG，该职位受审计部门委派，由总统任免，与政府各部门相独立），从而确保了评估报告的可靠性。

OMB会在每年夏季发布本财年的报告指南，近年来还特别针对各部门负责人和总检查长分别制定了报告模版，要求各部门在9月之前提交负责人和总检查长的报告。根据这些报告，OMB将撰写联邦政府信息安全状况的总报告，提交国会审议。

除OMB提交的总报告外，社会各界还可以看到另外一份电子政府信息安全评估报告，这就是电子政府信息安全评分表。不同的是，前者由作为政府组成部分的OMB做出，而后者则由国会众议院政府改革委员会做出。电子政府信息安全评分表的基础数据来源也是各部门提交的报告，但其评价方法是量化的。政府改革委员会特地制定了一套电子政务信息安全指标体系，评分后可以直观地了解政府各部门电子政府信息安全的基本情况。2005年以前，这套指标体系尚未成熟，一直没有公开，只能查询到各部门最终得分情况。在本次公开的资料中，已经可以看到包括指标体系在内的全部资料。

2、2005财年电子政务信息安全评分结果

电子政务信息安全评分表的结构比较简单，其背后则是几经改进并逐步稳定下来的一套科学的指标体系。表1显示了自GISRA和FISMA先后颁布以来国会对政府各部门的评分结果。

表1说明，政府各部门的安全状况在不断改进，虽然绝大多数部门在2001和2002财年得分不及格（等级为F），但自2003财年开始，24个部门的平均分已经超过及格线，并发展到D+。而且，在2005财年，有若干个单位得到了A或A+的好成绩，甚至有一个单位得到了满分。

但表1也同时暴露出了一些非常严峻的问题。2005财年，仍有8个部门的信息安全等级为F，其中竟然有国防部、能源部、国土安全部、国务院这4个敏感部门。因此，众议院公布本次的评分结果后，对这些部门的批评便一直不断。

表1 2001-2005财年各部门评分结果

部门	2005财年		2004财年		2003财年		2002财年		2001财年	
	分数	等级	分数	等级	分数	等级	分数	等级	分数	等级
农业部	24	F	49.5	F	40	F	36	F	31	F
国际发展局	100	A+	99	A+	70.5	C-	52	F	22	F
商务部	67	D+	56.5	F	72.5	C-	68	D+	51	F
国防部*	38.75	F	65	D	65.5	D	38	F	40	F
教育部	71	C-	76.5	C	77	C+	66	D	33	F
能源部	46.75	F	48.5	F	59.5	F	41	F	51	F

环境保护局 97.5 A+ 84 B 74.5 C 63 D- 69 D+
总务管理局 92.5 A- 79.5 C+ 65 D 64 D 66 D
卫生和公众服务部 45.5 F 49.5 F 54 F 61 D- 43 F
国土安全部 33.5 F 20.5 F 34 F -- -- -- --
住房和城市发展部 67.5 D+ 28 F 40 F 48 F 66 D
内务部 41.5 F 77 C+ 43 F 37 F 48 F
司法部 66.5 D 82.5 B- 55.5 F 56 F 50 F
劳工部 99 A+ 83 B- 86.5 B 79 C+ 56 F
国家宇航管理局 80 B- 60 D- 60.5 D- 68 D+ 70 C-
原子能管理委员会 60.5 D- 88 B+ 94.5 A 74 C 34 F
国家科学基金会 95 A 77.5 C+ 90.5 A- 63 D- 87 B+
人事管理办公室 98 A+ 72.5 C- 61.5 D- 52 F 39 F
小型商业管理局 78 C+ 60 D- 71 C- 48 F 48 F
社会安全管理局 99 A+ 86 B 88 B+ 82 B- 79 C+
国务院 37.5 F 69.5 D+ 39.5 F 54 F 69 D+
运输部 71.5 C- 91.5 A- 69 D+ 28 F 48 F
财政部* 60.5 D- 68 D+ 64 D 48 F 54 F
退伍军人事务部* 46 F 50 F 76.5 C 50 F 44 F
平均分 67.4 D+ 67.3 D+ 65 D 55 F 53 F

3、指标体系评分方法和内容概述
政府改革委员会采取的评分方法与OMB每财年向联邦政府各部门下发的报告指南密切相关。OMB要求各部门回答的问题中，绝大多数都是以百分比作为考量。某项工作的得分与该工作在单位内实施的范围成正比，满分则为100。例如，0分表示比例小于最低要求，例如只有29%甚至更低比率的雇员接受过安全培训。不同的比例范围将被赋予不同的分数，总分数则由各单项分数汇总而成。最后，根据总分评出24个部门各自的级别。
总分与等级的对应如下：
90到93 = A-，94到96 = A，97到100 = A+
80到83 = B-，84到86 = B，87到89 = B+
70到73 = C-，74到76 = C，77到79 = C+
60到63 = D-，64到66 = D，67到69 = D+
59及59分以下= F
表2显示了2005财年的详细评分内容。该表主要由6部分组成，因篇幅所限，表2中只详列了前两部分的内容。
需要指出，为求完善，OMB一直在通过更新每财年的报告指南来改进这些评分项目和赋值权重，所以各年度的评分内容稍有不同，但OMB同时也在极力确保各财年之间结果的一致性和可比性。
表2 2005财年评分内容
评分要点 得分
A.年度测试 20
1.被检查的信息系统所占比例 1).本部门对多少信息系统进行过检查 高影响级系统 6
90-100% 6
75-89% 4
60-74% 2
45-59% 0.5
44%及以下 0
中影响级系统 3
90-100% 3
75-89% 2
60-74% 1
45-59% 0.5
44%及以下 0
低影响级系统 1
96-100% 1
51-95% 0.5
50%及以下 0
2).合同商对多少系统操作过程和设施进行过检查 高影响级系统 6
90-100% 6
75-89% 4
60-74% 2
45-59% 0.5
44%及以下 0
中影响级系统 3
90-100% 3
75-89% 2
60-74% 1
45-59% 0.5
44%及以下 0
低影响级系统 1
96-100% 1
51-95% 0.5
50%及以下 0
3).是否对合同商使用或运行的系统依照有关政策和指南进行了检查 96-100%（不扣分） -0
51-95%（A.1得分扣除50%） -50%
50%及以下（A.1得分全部扣除） -100%
B.行动和里程碑计划（POA&M） 15

2.本部门是否制定了整个部门范围内的行动和里程碑计划 1).POA&M是整个部门范围内的过程，考虑了信息系统中所有已知的安全不足 几乎总是，即96-100%的时间 3
大部分时间是，即81-95%的时间 2
经常是，即71-80%的时间 1
有时是，即51-70%的时间 0.5
很少，即50%及以下的时间 0
2).当发现安全不足时，有关人员要为其系统制定、实施和管理POA&M 几乎总是，即96-100%的时间 4
大部分时间是，即81-95%的时间 2
经常是，即71-80%的时间 1
有时是，即51-70%的时间 0.5
很少，即50%及以下的时间 0
3).有关人员是否经常就信息安全补救工作的情况向首席信息官汇报 几乎总是，即96-100%的时间 1
经常是，即51-95%的时间 0.5
很少，即50%及以下的时间 0
4).首席信息官是否每季度跟踪、维护和检查POA&M活动 几乎总是，即96-100%的时间 2
大部分时间是，即81-95%的时间 1.5
经常是，即71-80%的时间 1
有时是，即51-70%的时间 0.5
很少，即50%及以下的时间 0
5).总检查长的发现是否纳入了POA&M过程中 几乎总是，即96-100%的时间 2
经常是，即51-95%的时间 1
很少，即50%及以下的时间 0
6).是否对所发现的安全不足的紧要程度进行了排列 几乎总是，即96-100%的时间 3
大部分时间是，即81-95%的时间 2
经常是，即71-80%的时间 1
有时是，即51-70%的时间 0.5
很少，即50%及以下的时间 0
C.认证和认可（C&A） 20
3.信息系统安全认证和认可 1).经过认证和认可的系统比例 （略） 12
2).其安全控制在一年内经过测试和评估的系统比例 （略） 4
3).其应急计划经过演练的系统比例 （略） 4
D.配置管理 20
4.配置管理 是否有覆盖整个部门的配置策略 （略） 20
E.事件检测和响应 15
事件检测和响应 1).是否有记录在案的事件检测和报告流程 （略） 7
2). 是否有记录在案的向执法机构的报告流程 （略） 4
3).是否有向US-CERT报告的流程 （略） 4
F.培训 10
是否能确保包括合同商在内的所有人员均受到信息安全培训 1).机构的雇员（包括合同商）接受培训的比例 （略） 4
2).具有高级安全知识的雇员 （略） 4
3).2005财年是否提供了足够的培训经费 （略） 1
4).是否在安全意识培训、道德培训或其它培训中解释了对等文件共享政策 （略） 1

4、评分结果反映的主要问题

针对这套指标体系的评分结果，政府改革委员会总结出了联邦政府电子政府信息安全存在的以下不足：

（1）年度测试

某些部门还有大量系统没有进行分类；虽然大多数部门对应急计划的演习做出了积极努力，但仍有若干部门对高影响级系统应急计划的演习比例低于60%。

（2）配置管理

大多数部门已经开始制定或已经实施了配置管理策略，但其中一些部门的实施水平较低。

（3）事件报告

各部门的事件报告工作很不理想。一些部门甚至没有报告任何安全事件，一些部门报告的安全事件则比USCERT掌握的一半还要低。

（4）培训

虽然大多数部门已经对雇员实施了安全培训，但安全岗位上的人员还普遍缺乏专门的训练。

（5）信息系统清单

有相当多的部门没有制定主要IT系统的清单。

5、结语

美国电子政府信息安全评分制度本身属于一种较宏观的风险评估形式，具有很强的系统性特点。其指标体系充分依赖了此前已经开展的基础工作，例如NIST发布的800-26、800-37、800-53等。从评分结果看，美国联邦政府各部门的信息安全状况在2001年和2002年普遍没有达到及格线，但这并不等于其电子政务安全“不堪一击”，而是反映出主管部门在当时尚未就信息安全自评估、认证认可、应急处理、培训等工作做出统一、明确的规定。自从FISMA、FIPS 199、800-53系列等法规、标准和指南发布后，这种局面已大为改观。评分表上，近三年成绩的稳固增长已经有了很强的说服力。由此可见，一套行之有效的信息安全指标体系必须建立在牢固的信息安全基础性工作之上。指标体系的制定，也要具备合适的时机。

回到目录

上篇文章 美国电子政务项目管理应用现状分析 2006-7-18 10:49:02

下篇文章 美国电子政务考察报告 2006-6-13 13:44:02