中国政府部门网络安全保护研究

陈彦达[1]，丁韦娜[2]，王伟楠[3]
（1. 审计署审计科研所，北京 100086；
2. 国家科技风险开发事业中心，北京 100036；
3. 中国科学技术发展战略研究院，北京 100038）

摘 要：本文针对目前中国政府部门机构网络安全保护存在的问题，借鉴美国联邦政府网络安全保护经验，提出了中国政府应着力从网络安全等级保护与关键信息基础设施重点保护的实施标准框架构建、政府网络安全风险管理流程标准和指南制定、政府网络安全风险报告与监测和评估机制完善、政府网络安全人才队伍建设、政府网络安全审计监督相关法律法规修订这五个方面加强网络安全保护工作。

关键词：政府网络；安全保护；基础设施；风险管理
中图分类号：F26 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2020.10.007

习近平总书记指出，“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”。中国政府部门越来越依赖信息系统和网络开展业务，海量业务数据、机密数据、公民数据在政府信息系统和网络之间传输、交换、存储。因此，政府部门的网络对于世界范围内的情报部门和网络中恶意行动者有很强的吸引力，所面临的网络安全风险①远高于其他机构的风险。政府网络安全具有复杂性、系统性、动态变化性、专业性②，保护政府网络安全是一项复杂、专业、系统的工作。随着互联网、大数据、云计算的发展，相对分散的网络融合成为深度关联的整体，网络攻击传播速度更快、影响范围更广、产生的损失更大[1]，对信息安全提出了更高的要求[2]，可以认为网络安全是信息安全发展的高级阶段③。

1 中国政府机构网络安全保护现状及存在的问题

2017 年 6 月，中国网络安全领域的基础性法律《中华人民共和国网络安全法》（以下简称《网络安全法》）[3] 正式实施，为中国有效应对网络安全威胁和风险、开展保障网络安全等工作提供了上位法依据，这表明我国网络安全保护工作取得了丰

第一作者简介：陈彦达（1981—），女，副研究员，博士，主要研究方向为金融监管、网络安全风险、金融科技。
通讯作者简介：丁韦娜（1986—），女，助理研究员，博士后，主要研究方向为科技管理，区域经济。邮箱：dwn9534@163.com
项目来源：科技部科技创新战略研究专项“决胜进入创新型国家关键问题与对策研究”（ZLY201951a）。
收稿日期：2020-08-03

① 网络安全风险：可表示为对网络安全目标（网络数据的完整性、保密性、可用性）的不确定性影响，利用信息资产或信息组的脆弱性产生的利用信息资产或信息组的脆弱性产生的特定威胁以及由此可能给组织带来的其他损害。

② 政府信息系统和网络高度复杂，种类繁多，技术多样，在地理上是分散的，专业技术人员水平参差不齐，这增加了识别、管理和保护网络和信息安全的难度。此外，政府信息系统和网络通常与其他内外部系统和网络（包括互联网）相互连接，网络攻击渠道复杂，扩大了网络攻击的影响面。

③ 一方面网络安全拓展了传统信息安全的内涵，不仅仅关注信息系统的安全，还要关注网络安全基础设施、云、移动互联网、物联网、工业控制系统、大数据安全等系统或平台；另一方面信息安全等级保护法律法规和标准需要升级为网络安全等级保护。

硕的成果。但中国政府网络安全保护在落地实施过程中，仍存在一些问题。

1.1 《网络安全法》明确了中国网络安全监管职责和分工的总体原则，但部分政府网络安全具体管理机制尚待完善

《网络安全法》中明确了中国网络安全监管职责和分工的总体原则，但是具体的政府网络安全管理机制还需要在《网络安全法》的配套法律法规中予以明确，如建立政府网络安全风险报告与评估监测机制、建立对政府网络安全保护和监管工作的独立第三方监督机制等。

《网络安全法》中规定，国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。目前，中国国家互联网应急中心负责收集网络攻击事件和安全威胁信息，关注的是外部网络攻击事件，尚未收集网络攻击损失信息。政府网络安全内部风险的收集、报告、监测和评估机制仍需完善，监管机构存在无法及时发现政府网络安全保护工作的问题及难点的风险。政府网络安全管理工作是否落实了《网络安全法》及配套制度文件的要求、政府网络安全保护和监管职责履行、政府网络安全资金绩效审计均属于审计机关职责范围。近年来审计机关一直在探索政府信息系统审计和网络安全审计实践[①]，已经积累了相关的审计经验。但是《网络安全法》及《网络安全等级保护条例（征求意见稿）》[②]并未明确国家审计对政府网络安全保护和监管工作的独立第三方监督职责。

1.2 网络安全等级保护、关键信息基础设施重点保护落地实施相关的法律法规和标准体系亟待完善

等级保护制度筑起了中国网络和信息安全的重要防线。中国《网络安全法》构建了网络安全等级保护制度（等保 2.0），这表明《信息安全等级保护管理办法》及《信息系统安全等级保护定级指南》确定的“信息安全等级保护”（等保 1.0）已全面升级。

从国家标准化管理委员会工作来看，网络安全等级保护、关键信息基础设施重点保护落地相关的

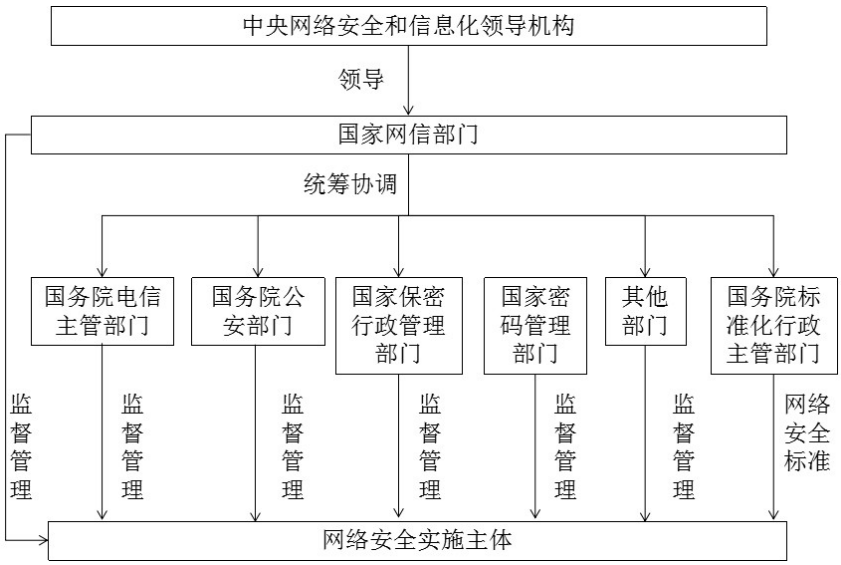

图 1　中国网络安全监管框架

资料来源：《网络安全法》《网络安全等级保护条例（征求意见稿）》。

① 审计机关近年来依托预算执行审计、政策跟踪审计以及审计调查探索政府信息系统和网络安全审计实践。

② 2018 年 6 月 27 日，公安部会同有关部门起草了《网络安全等级保护条例（征求意见稿）》，在三十三条中明确了行政主管部门对网络运营者网络安全等级保护进行审计审核。第六章明确了县级以上公安机关和行业主管部门在网络安全等级保护方面的监督管理职责。但在征求意见稿中未明确对网络安全等级保护监督管理的独立第三方监督。

表 1　信息和网络安全保护相关标准

分类	标准名称	标准号	类别	状态	发布日期	实施日期
信息安全保护要求	计算机信息系统安全保护等级划分准则	GB/T 17859-1999	强标	现行	1999/09/13	2001/01/01
	信息安全技术 信息系统安全管理要求	GB/T 20269-2006	推标	现行	2006/05/31	2006/12/01
	信息安全技术 网络基础安全技术要求	GB/T 20270-2006	推标	现行	2006/05/31	2006/12/01
	信息安全技术 信息系统通用安全技术要求	GB/T 20271-2006	推标	现行	2006/05/31	2006/12/01
信息系统安全等级保护	信息安全技术 信息系统安全等级保护基本要求	GB/T 22239-2008	推标	现行	2008/06/19	2008/11/01
	信息安全技术 信息系统安全等级保护定级指南	GB/T 22240-2008	推标	现行	2008/06/19	2008/11/01
	信息安全技术 信息系统安全等级保护实施指南	GB/T 25058-2010	推标	现行	2010/09/02	2011/02/01
	信息安全技术 信息系统安全等级保护测评要求	GB/T 28448-2012	推标	现行	2012/06/29	2012/10/01
	信息安全技术 信息系统安全等级保护测评过程指南	GB/T 28449-2012	推标	现行	2012/06/29	2012/10/01
网络安全等级保护	信息安全技术 网络安全等级保护定级指南			已发征求意见稿		
	信息安全技术 网络安全等级保护基本要求	GB/T 22239-2019	推标	即将实施	2019/05/10	2019/12/01
	信息安全技术 网络安全等级保护实施指南			制定中		
	信息安全技术 网络安全等级保护测评要求	GB/T 28448-2019	推标	即将实施	2019/05/10	2019/12/01
	信息安全技术 网络安全等级保护测评过程指南	GB/T 28449-2018	推标	现行	2018/12/28	2019/07/01
关键信息基础设施网络安全重点保护	信息安全技术 关键信息基础设施网络安全框架			制定中		
	信息安全技术 关键信息基础设施网络安全保护基本要求			已发布征求意见稿		
	信息安全技术 关键信息基础设施安全检查评估指南			已发布征求意见稿		
	信息安全技术 关键信息基础设施安全保障指标体系			已发布征求意见稿		
政府部门信息安全	信息安全技术 政府部门信息安全管理基本要求	GB/T 29245-2012	推标	现行	2012/12/31	2013/06/01
	信息安全技术 政府门户网站系统安全技术指南	GB/T 31506-2015	推标	现行	2015/05/15	2016/01/01
	基于云计算的电子政务公共平台安全规范 第 1 部分：总体要求	GB/T 34080.1-2017	推标	现行	2017/07/31	2017/11/01
	基于云计算的电子政务公共平台安全规范 第 2 部分：信息资源安全	GB/T 34080.2-2017	推标	现行	2017/07/31	2017/11/01

资料来源：根据国家标准化管理委员会公布的资料整理，统计时间截至 2019 年 6 月 30 日。

规定和标准部分尚处于起草、征求意见、即将实施阶段，这表明网络安全等级保护、关键信息基础设施重点保护落地实施的制度化体系尚未完全建立。

1.3 政府网络安全保护能力参差不齐

政府机构在网络安全威胁[①]理解、网络安全意识、网络安全需求、网络安全资金预算、网络安全风险管理实践经验、网络安全人才队伍等方面存在差异，因而政府网络安全保护能力参差不齐。比如有的政府机构电子政务采用了分布式架构的云平台，有的政府机构电子政务采用了传统中心服务器的方式，这两种方式面临不同的网络安全威胁，对网络安全保护能力要求也是不同的，采用云平台的网络安全保护能力要求更高。

1.4 政府网络安全风险管理流程的标准和指南缺乏

由于政府网络安全保护能力参差不齐，迫切需要国家制定标准化的政府网络安全风险管理流程标准，应用风险管理的原则和最佳实践来提高政府关键基础设施和网络的安全性和恢复能力。中国在关键信息基础设施和网络的安全保障体系建设方面起步较晚，还未制定政府网络安全的风险生命周期管理（识别风险、管理风险、降低风险）流程和标准，缺乏对政府网络安全保护落地实施的指导。

1.5 政府网络安全人才短缺，政府网络安全管理组织结构还需完善

网络安全的竞争，归根结底是人才竞争。政府网络安全人才短缺现象严重。中国信息安全测评中心等单位发布的《2018 网络安全人才发展白皮书》显示，事业单位和政府机构 / 非营利机构的网络安全人才仅占网络安全从业人数的 4.75%。

《信息安全技术 政府部门信息安全管理基本要求》（GB/T 29245-2012）要求建立信息安全责任制和相关工作机制，政府部门需要指派一名领导主管本单位信息安全管理工作，结合单位实际情况制定完善信息安全管理制度，完善技术防护流程并处理重大信息安全事件；应指定一个机构承担并开展相关信息安全管理工作；各内设机构应指派专职或兼职信息安全员，负责日常信息安全督促、检查等管理工作。由于网络安全管理既是业务职能又是 IT 职能，如果政府机构没有设置信息技术领导，从技术上保证政府机构落实网络安全保护要求存在一定的风险。

2 美国联邦政府网络安全保护经验

美国非常重视网络安全问题，在网络安全保护方面积累了丰富的经验，虽然与中国的体制和国情不同，但仍有不少科学管理做法值得借鉴，如联邦政府网络安全保护的法律体系、职责分工、网络安全风险管理实施指南、风险监测评估、审计监督等方面。

2.1 通过法律体系明确保护联邦网络和系统的战略和方法，以及联邦政府网络安全职责分工

美国联邦政府网络安全法律体系提供了有效保护联邦信息和 IT 资产的全面框架，并明确要求美国审计署对联邦机构信息和网络安全工作进行审计评估，其核心法律是 2002 年《联邦信息安全管理法案》（FISMA 2002）和 2014 年《联邦信息安全现代化法案》（FISMA 2014）。

表 2 的法律体系明确联邦政府网络安全保护职责，包括联邦政府网络安全保护实施主体职责、监管职责。每一个联邦机构都负责自己的网络安全工作。在指导、支持、监督其他部门实施的网络安全实践方面，美国管理与预算办公室（OMB）、美国国家标准与技术研究院（NIST）、美国国土安全部（DHS）、美国总务署（GSA）发挥了跨部门作用[5]，美国审计署发挥了外部监督作用。每个联邦机构运用风险管理方法保护本机构的信息和网络安全。

2.2 发布联邦政府网络安全风险管理实施指南，积极推进网络安全保护落地实施

美国联邦政府网络安全监管机构向各联邦机构提供了网络安全风险管理操作指南，在识别风险、管理风险、降低风险等生命周期环节提供指导。图 3 为联邦政府网络安全生命周期管理指南，其中美国国家标准与技术研究院网络安全框架最为关键。

2014 年美国国家标准与技术研究院发布了美

① 威胁：可能对系统或组织造成危害的不期望事件的潜在源由。

表 2　美国联邦政府网络安全法律法规梳理

法律法规名称	发布年份	主要内容
《联邦信息安全管理法案》	2002	明确了联邦政府网络安全保护的角色和职责，并要求各联邦机构制定、记录和实施信息安全计划
《联邦信息安全现代化法案》	2014	修改了 2002 年法律，以澄清、更新管理与预算办公室、国土安全部对联邦机构信息安全的管理职责和权限
《国家网络安全保护法案》	2014	正式建立国土安全部的国家网络安全、通信集成中心，连接联邦机构及非联邦实体共享信息
《联邦网络安全增强法》	2014	正式更新了国家标准技术研究所的职能，包括确定和开发关键基础设施所有者和运营商自愿使用的网络安全风险框架
《联邦网络安全增强法》	2015	要求通过使用联邦入侵预防和检测能力计划（爱因斯坦计划）来保护联邦网络
《加强联邦网络和关键基础设施的网络安全》	2017	要求各联邦机构利用国家标准技术研究所出台的《关键基础设施网络安全框架》规则来管理联邦机构的网络安全风险

资料来源：根据美国联邦政府网络安全法律法规整理。

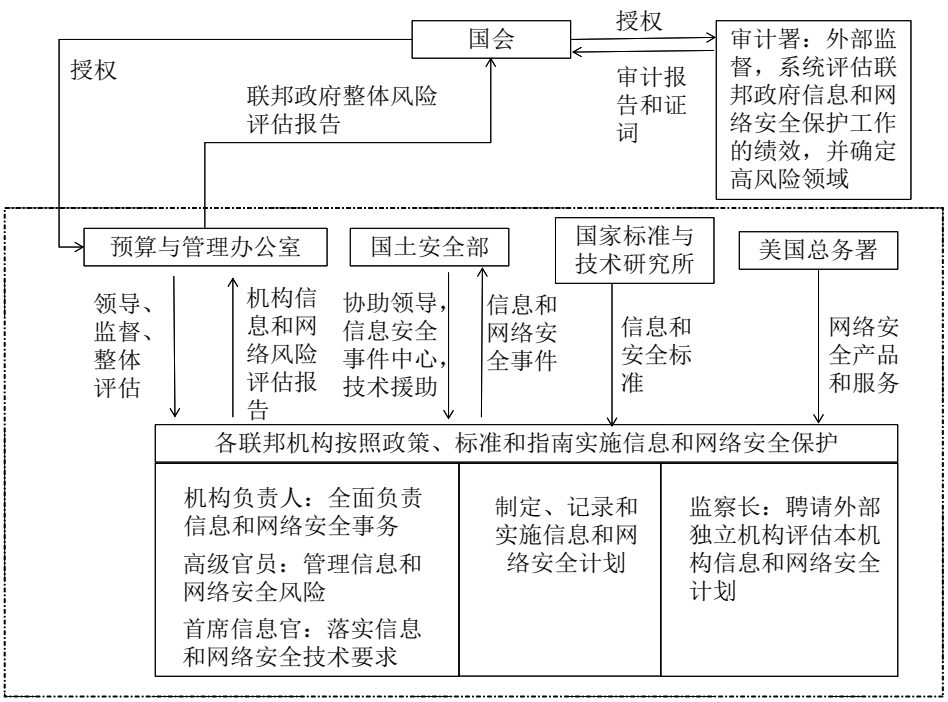

图 2　联邦政府网络安全保护职责划分

资料来源：根据美国审计署审计报告整理[4]。图中虚线方框为美国审计署审计范围。美国对于网络安全与信息安全并未明确区分，本图中统一处理为信息和网络安全。

国国家标准与技术研究院网络安全框架 1.0[7]。这是一套基于安全风险、应用于关键基础设施领域的网络安全风险管控的流程，也可视为关键基础设施网络安全风险管控的标准化实施指南，旨在

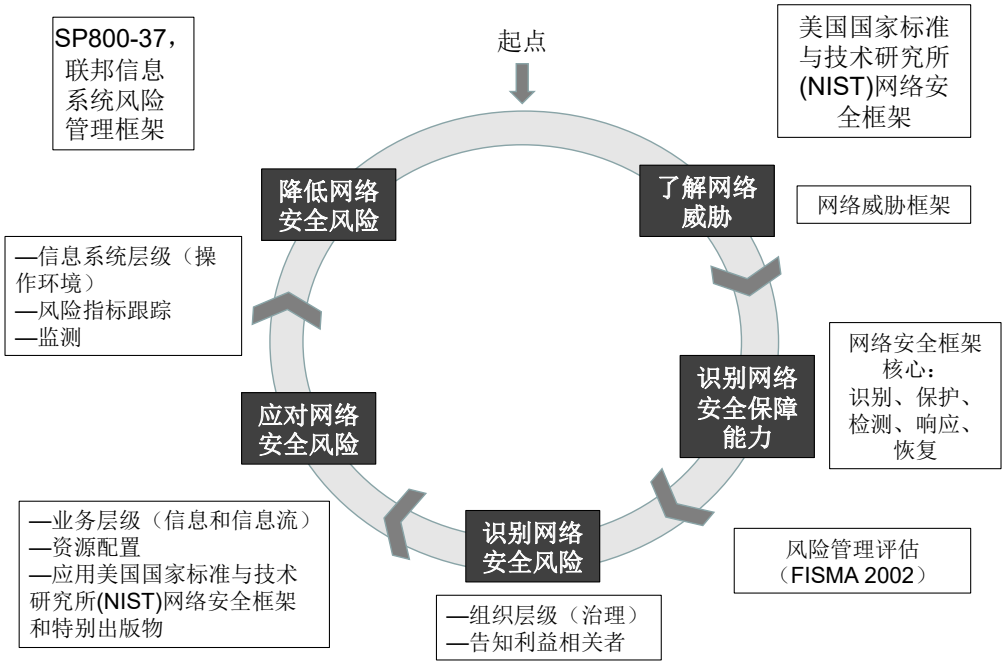

图 3　联邦政府网络安全生命周期管理指南 [6]

帮助联邦机构应用风险管理的原则和最佳实践来提高关键基础设施的安全性和恢复能力。2018 年 4 月发布了美国国家标准与技术研究院网络安全框架 1.1，增加了网络供应链风险管理的内容。

美国国家标准与技术研究院网络安全框架有 5 个核心安全功能：识别、保护、检测、响应和恢复。

（1）识别。

识别能力是有效使用网络安全框架的基础。了解业务内容、支持关键职能的资源以及相关的网络安全风险，使组织能够根据其风险管理战略和业务需求优先考虑网络安全工作。这个功能细化的例子包括资产管理和授权、全面风险管理。

（2）保护。

制定、实施恰当的保障措施，确保能够提供关键基础设施服务，并提供限制或阻止潜在网络安全事件影响的功能。细化的例子包括远程访问保护、认证和授权、网络保护。

（3）检测。

制定、实施恰当的措施来识别并及时发现出可能发生的网络安全事件。细化的例子包括反网络钓鱼功能、恶意软件防御能力、其他防御能力。

（4）响应。

制定、实施恰当的措施来对检测到的事件采取必要的行动，并提高控制潜在网络安全事件影响的能力。细化的例子包括计划和流程，评估和改进。

（5）恢复。

制定、实施恰当的活动，以恢复因安全问题而受损的相关功能或服务，并支持及时恢复到正常操作，以减轻网络安全事件的影响。细化的例子包括规划和测试、受影响的个人处理流程、备份能力。

应对网络安全风险，需要持续地执行这 5 个核心功能。5 个功能向组织提供了一个网络安全风险管理生命周期的高级战略视图。5 个功能中共有 23 个类别和 108 个子类别。

2.3　对联邦政府网络安全风险进行监测和评估

各联邦机构监察长负责聘请外部评估机构来评估本机构信息和网络安全计划实施情况，频率至少每年一次。各联邦机构应当每年向管理与预算办公室提交本机构信息和网络安全风险管理报告，并报告本机构的《联邦信息安全管理法案》

指标信息（首席信息官指标[①]和监察长指标[②]）。管理与预算办公室和国土安全部将通过《联邦信息安全管理法案》指标评估各联邦机构的网络安全风险，并向总统汇总报告联邦政府整体网络安全风险评估。管理与预算办公室、国土安全部通过评估汇总信息，可以确定网络安全新技术需求和政府服务整合领域，以改善政府机构的网络安全态势。

《联邦信息安全管理法案》指标旨在确保联邦机构信息技术安全的最低门槛，联邦机构还需采用更多的措施和方法来管理风险。24 个首席财务官法案机构[③]至少每季度报告 1 次《联邦信息安全管理法案》指标。所有非首席财务官法案机构[④]（即小型和独立机构）至少每半年报告 1 次《联邦信息安全管理法案》指标。

2.4 美国审计署对联邦政府网络安全进行监督

联邦政府网络安全法律法规要求美国审计署定期进行网络安全审计，并向参议院和众议院相关委员会提交审计报告和证词。2017—2018 年美国审计署网络安全相关的审计报告主要分为 4 个系列：关键基础设施、网络安全、信息安全、高风险。关键基础设施审计，评估关键基础设施部门应用美国国家标准与技术研究院网络安全框架的程度[10]。网络安全审计，不仅评估各联邦机构网络安全政策和方法的合法性、充足性和有效性（包括评估美国国家标准与技术研究院网络安全

表 3 美国联邦政府网络安全审计评估指标示例[14]

序号	识别功能中资产管理和授权的要求	评估依据
1	企业级硬件资产自动化库存管理能力（例如扫描 / 设备发现过程）所覆盖的政府硬件资产	联邦信息安全管理法案首席信息官指标，1.2、1.4
2	企业级软件资产自动化库存管理能力（例如扫描 / 设备发现过程）所覆盖的政府软件资产	联邦信息安全管理法案首席信息官指标，1.2.1、1.2.2、1.5
3	组织的非保密网络拥有一种技术解决方案，用于检测和警告未经授权的硬件资产的连接	联邦信息安全管理法案首席信息官指标，3.16
4	检测、警报或阻止未授权软件执行，需要包含组织的端点和移动资产	联邦信息安全管理法案首席信息官指标，3.17
5	组织的非保密系统能防范账号劫持	联邦信息安全管理法案首席信息官指标，1.1.1、1.1.2、1.1.3
6	基于信息泄露对运营、资产、个人、其他组织以及国家的风险持续对信息系统进行授权	联邦信息安全管理法案监察长指标，1.1.11

① 预算与管理办公室和国土安全部负责制定《联邦信息安全管理法案》首席信息官指标。《联邦信息安全管理法案》首席信息官指标一方面可以确保各机构执行联邦政府优先考虑事项；另一方面向预算与管理办公室提供绩效数据。2016 年以来，预算与管理办公室和国土安全部按照美国国家标准与技术研究院网络安全框架的 5 个功能重新组织了《联邦信息安全管理法案》首席信息官指标结构。《联邦信息安全管理法案》首席信息官指标示例：企业级软件资产自动化库存管理能力所覆盖的终端数量[8]。

② 预算与管理办公室、国土安全部、监察长理事会、联邦首席信息官理事会共同协商制定《联邦信息安全管理法案》监察长指标。《联邦信息安全管理法案》监察长指标结构按照美国国家标准与技术研究院网络安全框架的 5 个功能组织。《联邦信息安全管理法案》监察长指标提供了检测和评估机构信息和网络安全计划和实践有效性的指导，该指标评估的最终结果体现为 5 个层级的网络安全控制水平：非制度化、制度化但实施未统一、统一实施但缺乏定性和定量的指标、可管理和可监测、最优。《联邦信息安全管理法案》监察长指标示例：组织是否制定了风险管理计划，政策和程序是否符合《联邦信息安全管理法案》要求、美国管理与预算办公室政策和适用的美国国家标准与技术研究院指南[9]。

③ 首席财务官法案机构是接受预算管理办公室监管的 24 个美国联邦部门。这些部门需要报告信息安全数据，供国土安全部、预算与管理办公室和国会用于监测和跟踪。

④ 非首席财务官法案机构包括小型（6 000 名雇员）、微型（100 名雇员）部门以及一些较大的，通常是独立的监管机构。

框架应用程度），还要评估管理与预算办公室、国土安全部、国家标准与技术研究院促进联邦机构信息和网络安全保护工作的有效性[11]。信息安全审计，依据《联邦信息系统控制审计手册》（FISCAM）①开展，对各联邦机构信息系统控制的有效性和安全性进行评估[12]。自20世纪90年代初以来，美国审计署开展了一个政府高风险项目，报告在政府运营中存在欺诈、浪费、滥用、管理不善等风险的领域，并报告政府在面临经济、效率挑战时应进行转型的领域。通常在每届新国会启动时，美国审计署向国会报告高风险领域的处理进展情况，并更新高风险清单。美国审计署于1997年首次将信息安全确定为政府范围内的高风险领域。随后，2003年将信息安全高风险领域扩展到保护网络关键基础设施[13]，2015年将信息安全高风险领域扩展到保护个人身份信息隐私。高风险领域审计关注的是联邦政府所面临的整体、共性的高风险问题。

3 中国政府网络安全保护建议措施

根据当前中国政府网络安全保护存在的问题，结合美国联邦政府网络安全保护经验，中国政府网络安全保护应重点关注以下5个方面。

（1）完善网络安全等级保护、关键信息基础设施重点保护落地实施相关法律法规和标准体系。

虽然中国《网络安全法》明确了网络安全等级保护制度和关键信息基础设施重点保护制度，但其落地实施相关的法律法规和标准体系亟待完善。从信息安全等级保护升级到网络安全等级保护，安全保护对象和要求进行了扩展和升级。虽然等级保护制度始终保持不变的安全保护目标（保护系统安全、保证敏感信息的处理、保证服务的连续），但是等级保护的对象、方法、流程都有所不同②，因此政府网络安全保护应进一步完善网络安全等级保护、关键信息基础设施重点保护落地实施相关法律法规和标准体系。

（2）制定政府网络安全风险管理流程标准和指南。

从美国联邦政府网络安全保护来看，美国国家标准与技术研究院网络安全框架起到了核心作用，既为联邦政府网络安全提供了实施指南，又为联邦政府网络安全评价提供了逻辑框架，保证了联邦政府网络安全工作之间的衔接和一致性。联邦政府网络安全评估监测指标《联邦信息安全管理法案》首席信息官指标和《联邦信息安全管理法案》监察长指标都是按照美国国家标准与技术研究院网络安全框架来组织的。美国国家标准与技术研究院网络安全框架、《联邦信息安全管理法案》首席信息官指标、《联邦信息安全管理法案》监察长指标系统性地回答了网络安全保护怎么做、做了哪些、做得怎么样这三个问题。

中国政府机构的网络安全保护能力参差不齐，更需要网络安全保护的操作指引，因此政府主管部门应从制定政府网络风险管理流程标准和指南入手，搭建包含识别、保护、检测、响应和恢复5个功能的政府网络安全框架，为中国政府网络安全保护工作落地实施提供指导。

（3）完善中国政府网络安全风险报告、监测和评估机制。

美国从2014年开始构建了一套完整的联邦政府网络安全工作监测和评估指标，即《联邦信息安全管理法案》首席风险官指标和《联邦信息安全管理法案》监察长指标，随后每年根据政府网络安全工作目标的变化修订这套指标。联邦政府

① 《联邦信息系统控制审计手册》是美国审计署根据公认政府审计标准执行信息系统控制审计的审计方法。该手册定义的5种控制类别包括：（1）访问控制，限制或检测对计算机资源的访问，保护它们免受未经授权的修改、丢失和泄露；（2）配置管理，防止对信息系统资源进行未经授权的更改，确保软件是最新版本，修补已知的漏洞；（3）职责分离控制，防止个人通过在两个或多个组之间的职责来控制流程的所有关键阶段；（4）应急计划控制，避免与计算机相关的操作出现重大中断；（5）安全管理控制，为确保理解风险和选择、实施和按预期运行有效控制提供框架。

② 信息安全等级保护的对象为信息和信息系统，网络安全等级保护扩展到基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据等多个系统平台。信息安全等级保护偏重于防护信息系统，而网络安全等级保护则要适应当前网络安全形势的发展，对于持续监测、威胁情报、快速响应提出了具体的落地措施。

网络安全风险监测和评估指标有利于监管机构评估联邦机构单个网络安全风险和整体网络安全风险，从而及时确定网络安全新技术需求和政府网络安全工作需要改进的地方。

中国政府网络安全从内部风险、外部风险两个方面完善网络安全风险报告、监测和评估机制。从外部风险来看，网络安全工作的系统性特点需要搭建国家层面的网络攻击历史数据库[15]，从公开渠道和监管机构尽可能多地收集和积累更加详细、一致、完整的有关网络攻击的报道和数据，特别是网络攻击的类型、频率和损失的数据，数据的精确性和完整性会对网络安全风险评估产生重要影响[16]；从内部风险来看，需要建立政府网络内部风险的收集、报告、监测、评估机制以及监测评估指标。

（4）加强政府网络安全人才队伍的建设和完善组织结构。

政府网络安全工作具有复杂性、系统性、动态变化性、专业性等特点，确保政府机构拥有充足的、具备相应技能的网络安全专业人员，并确保其全体员工了解信息安全责任，是政府网络安全面临的一大挑战。目前，中国已将网络安全作为一级学科，大力培养网络安全相关专业人才，但是政府网络安全人才仍存在短缺现象，政府主管部门应关注政府网络安全人才引进、培养等管理工作。网络安全管理既是一项业务职能又是一项 IT 职能，因此政府机构需要设置信息技术领导，专职负责确保政府机构落实有关信息和网络安全管理要求和技术要求。

（5）修订中国政府网络安全审计监督相关法律法规。

美国通过双层外部监督机制来推进联邦政府网络安全保护，从而保证网络安全评估的客观性和有效性。联邦政府派驻各机构的监察长每年负责聘请外部评估机构来评估机构网络安全。美国审计署作为外部监督机构，定期系统评估联邦政府信息与网络安全保护和管理工作的绩效。

为了保证中国网络安全评估的客观性和网络安全监管的有效性，需完善相关法规的修订，明确国家审计对政府网络安全保护和监管的独立第三方监督职责[16]。■

参考文献：

[1] 周文 . 整体保障关键信息基础设施网络安全 [N/OL].（2018-04-23）[2020-06-30]. http://theory.people.com.cn/n1/2018/0423/c40531-29944021.html.

[2] 王世伟，曹磊，罗天雨 . 再论信息安全、网络安全、网络空间安全 [J]. 中国图书馆学报，2016，42（225）：4-28.

[3] 人民网 . 中华人民共和国网络安全法 [N/OL].（2016-11-23）[2020-06-30]. http://cpc.people.com.cn/n1/2016/1123/c64387-28889083.html

[4] U.S. Goverment Accountability Office. Federal Information Security:Actions Needed to Address Challenges[R]. Washington: GAO, 2016.

[5] Kate Charlet. Understanding Federal Cybersecurity[R]. US Department of Defense, 2018.4.

[6] Office of Management and Budget. Federal Cybersecurity Risk Determination Report and Action Plan[R]. Washington: OMB, 2018.

[7] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity version 1.0[EB/OL]. (2014-02-14) [2020-06-30]. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-10.

[8] The Department of Homeland Security. FY 2018 CIO FISMA metrics (V2.0.1)[EB/OL]. (2018-05-01) [2020-06-30]. https://www.dhs.gov/sites/default/files/publications/FY%202018%20CIO%20FISMA%20Metrics_V2.0.1_final_0.pdf

[9] The Department of Homeland Security. FY 2016 inspector general federal information security modernization act of 2014 reporting metrics (V1.1.3) [EB/OL]. (2016-10-13) [2020-06-30]. https://www.dhs.gov/sites/default/files/publications/FY%202016%20IG%20FISMA%20Metrics%20508%20compliant%20.pdf.

[10] U.S. Goverment Accountability Office. Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework

Adoption[R]. Washington: GAO, 2018.

[11] U.S. Goverment Accountability Office. Cybersecurity: Threats Impacting the Nation[R]. Washington: GAO, 2012.

[12] U.S. Goverment Accountability Office. Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions[R]. Washington: GAO, 2018.

[13] U.S. Goverment Accountability Office. High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation[R]. Washington: GAO, 2018.

[14] Office of Management and Budget. Reporting guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[R]. Washington: OMB, 2017.

[15] 陈彦达，王玉凤 . IMF 金融机构网络风险量化评估框架对我国金融审计的启示 [J]. 中国审计，2019（11）：62-63.

[16] Antoine Bouveret. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment[R].Washington: IMF Working Paper, 2018.

Research on Government Cybersecurity Protection in China

CHEN Yan-da[1], DING Wei-na[2], WANG Wei-nan[3]

(1. National Science and Technology Venture Capital Development Center , Beijing 100038;

2. Audit Research Institution of National Audit Office of the People's Republic of China, Beijing 100036;

3. Chinese Academy of Science and Technology for Development, Beijing 100031)

Abstract: In view of current situation and existing problems of government cybersecurity protection in China, combining with practice of federal cybersecurity protection in USA, the paper puts forward five aspects that government cybersecurity audit should pay attention to in China: improving relevant laws and standards of network security level protection and key information infrastructure protection, making guidelines for government cybersecurity risk managements, improving reporting and monitoring mechanism of government cybersecurity risk, strengthening talent team construction of government cybersecurity, amending relevant laws and regulations of audit supervision for government cybersecurity.

Key words: government cybersecurity; security protection; base installation; risk management