新形势下政府行业信安保障工作新思路

政府事业部 陈安君 张智南

关键词：国家网络安全等级保护 关键信息基础设施 全态势感知 监测预警 网络安全人才

摘要：《中华人民共和国网络安全法》的颁布，构成了国家信息安全监管的新形势，由此带来网络和信息安全的保障，会在横向扩展和纵向深化两个维度上发生相应的变化，给政府行业信息安全保障工作提出新的任务和挑战。本文结合《网络安全法》的相关规定，梳理了安全监管新形势下政府单位信息安全保障工作的新思路。

《中华人民共和国网络安全法》内容涉及基本原则、网络安全战略、网络空间治理目标、网络安全监管体制及政府各部门职责权限、强化网络运行安全、重点保护关键信息基础设施、网络安全义务和责任、违法惩处、监测预警与应急处置措施等方面。《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法制建设的重要里程碑。

国家法律法规、监管职能部门、监管技术规范等方面的新变化，构成了国家信息安全监管的新形势，由此带来网络和信息安全的保障会在横向扩展和纵向深化两个维度上发生相应的变化，给政府行业信息安全保障工作提出新的任务和挑战。本文结合《网络安全法》的相关规定，梳理了安全监管新形势下政府单位信息安全保障工作的新思路。

第一：新的法律责任—需全面贯彻落实国家网络安全等级保护制度

《网络安全法》第二十一条规定，国家实行网络安全等级保护制度。作为我国首部网络安全专门性法律，首次以法律形式要求国家

实行网络安全等级保护制度，将等级保护制度从一项基本制度、基本国策上升到了法律层面。从中我们也可以看出国家对于等级保护制度全面贯彻的决心，后续各行各业尤其是政府部门对这一制度势必需要严格执行。此外根据网络安全法相关规定，我们也可以看出，网络安全法在原有信息系统安全等级保护制度的基础上，创新了网络安全等级保护的工作方法，各政府部门的信息安全建设需在原有信息系统安全等级保护制度建设的基础上，将新技术新应用带来的重要信息系统建设诸如云计算、移动互联、物联网、工业控制、大数据等领域的国家关键信息基础设施建设都纳入国家安全等级保护制度进行管理，将风险评估、安全监测、通报预警、应急演练、灾难备份、自主可控等重点措施也纳入了国家网络安全等级保护制度的管理范畴。需要注意的是：虽然许多单位已经按照原有的等级保护标准要求实施了安全防护，但在未来新修订的标准颁布后，需要按照修订后的标准要求，更新现有的防御体系，应用标准中新增的新型安全防护技术、方法，进一步增强系统的安全防护能力。

第二：新的监管维度—需对关键信息基础设施实施重点保护

网络安全法引入了新的监管维度——对关键信息基础设施实施重点保护。我们首先要识别当前纳入到关键信息基础设施范围的应用系统，如政府网站、重要平台、关系到国计民生的重要信息系统等。对于政府部门而言，在网络安全法即将颁布的一段时间内，需梳理《网络安全法》与现行法规之间的关系，明晰职责，建立健全相关配套标准；开启部门、行业、地方的立法和政策的制定、调整和完善相关工作；需对部门、行业内关键信息基础设施进行评估，对于容易受到网络侵害的关键行业要实施重点保护；对于负责运营的关键信息基础设施应设置专门安全管理机构和安全管理负责人，并对其进行安全背景审查，定期对从业人员进行安全意识培训、技术培训及技能考核，此外需对关键信息基础设施重要系统和数据库进行容灾备份。

第三：新的规则及义务—将个人信息保护提升到一定高度

本次出台的网络安全法聚焦个人信息保护，明确任何个人或组织不得窃取、篡改、损毁其收集的个人信息；网络安全运营者、网络安全产品和服务提供者的责任，不得窃取或者以其他非法方式获取个人信息，不得非法出售或非法向他人提供个人信息，并规定了相应的法律责任。

政府作为关系国计民生的重要行业，会在日常办公过程中收集到大量个人信息，随着网上办公便利的同时，个人信息泄露也成为政府部门面临的新挑战。本次网络安全法的出台，使得个人信息保护有法可依。这是我国以的法律形式要求各行业从事网络安全运维的单位和部门，要下大力气管好个人信息数据，这对涉及个人信息的政府行业相关部门提出了新考验。我们建议：针对涉及到使用、存储公民个人信息的政府单位，需尽快盘点已收集、使用、存储的个人信息的类型，对个人信息的载体处理分析、对使用个人信息的信息系统进行分析，积极打造个人信息的保护措施，完善单位及行业内的个人信息保护体系，将个人信息保护意识需提高到一个新高度。

第四：新的安全保障体系——建立健全以行业网络安全态势感知为技术基础的监测预警和应急处置体系

《网络安全法》第五章专门规定网络安全监测预警和应急处理制度建设，要求建立国家层面的网络安全监测预警和信息通报制度，强化网络安全事件风险防范机制，健全网络安全事件处置机制；要求从行业领域建立网络安全监测预警和信息通报制度。并要求网络运营者应当制定网络安全事件应急预案。

具体概括起来：各级相关政府机关需建设面向国家监管部门和行业所属单位的信息通报机制，建立感知网络安全状态的预警体系，判断安全风险发生发展趋势，对发生的安全问题及时进行预警通报和事件处置；此外各级政府部门还需建立健全网络安全事件应急工作机制，完善应急预案，定期组织演练，通过建立行业内监测预警与应急处置的制度和体系，从而提升整体的网络安全保护能力。

第五：新的战略举措—网络安全人才培养

《网络安全法》第二十条　国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

这是我国首次以法律条款的形式对网络安全领域的人才问题进行了规定。《网络安全法》的出台弥补了网络安全人才领域的法律空白，表明国家更加重视网络安全人才工作，更为以后政府及各个地方出台网络安全人才培养的细则提供了法律依据。

总的来说，《网络安全法》一方面明确规定了网络空间活动的法律禁区；另一方面对政府、企业等各行业都提出的更高要求。《网络安全法》的及时颁布，顺应了互联网时代的发展趋势，及时明确了网络空间行为的准则，有助于维护网络空间秩序，引领社会诚信，为政府、企业和个人网络空间的健康发展指明了方向，为依法治网和依法管网提供了法律依据，为我国拓展网络空间、规范建设网络强国、维护社会和谐稳定提供强有力的法制保障。

绿盟科技作为国家级应急响应支撑单位愿意利用自身的技术优势、人才优势，在政府行业党政机构、企事业单位的信息系统等级保护、电子政务外网、国家关键信息系统的风险管控、安全运维、网站监护、数据安全、态势感知、新一代威胁防护等方面为信息化建设保驾护航。