美军
网络安全试验鉴定

Cybersecurity Test and Evaluation

刘映国 编著

国防工业出版社
National Defense Industry Press

美军网络安全试验鉴定

刘映国　编著

国防工业出版社
·北京·

内 容 简 介

本书针对网络对抗愈演愈烈，武器装备面临网络安全威胁日趋严峻的态势，围绕美军近年来开展武器系统网络安全试验鉴定活动情况，系统分析研究了美军网络安全试验鉴定政策法规，组织实施流程规范，测试指标体系构建，网络试验靶场建设、网络安全评估与网络对抗人员培养等内容。从厘清概念与追溯源头入手，深入研究了信息系统、平台信息技术系统、风险管理框架与网络安全试验鉴定阶段划分、任务要求及相互之间关系。按照武器系统采办全寿命周期管理要求，梳理了网络安全试验鉴定在采办各阶段的任务及要求、组织实施责任机构，以及在采办决策中发挥的作用。

本书是一部注重理论方法探索与前瞻实践研究相结合的专著，适用于各级试验鉴定管理部门和组织实施机构领导与工程人员参考，也可作为网络安全评估与网络安全试验鉴定人员培训和相关专业教学的参考用书。

图书在版编目（CIP）数据

美军网络安全试验鉴定 / 刘映国编著. —北京：国防工业出版社，2018.4

ISBN 978-7-118-11545-1

Ⅰ. ①美… Ⅱ. ①刘… Ⅲ. ①计算机网络—网络安全—研究—美国 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2018）第 061741 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号　邮政编码 100048）

三河市众誉天成印务有限公司

新华书店经售

开本 710×1000　1/16　印张 23　字数 350 千字

2018 年 4 月第 1 版第 1 次印刷　印数 1—2500 册　定价 78.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010) 88540777　　发行邮购：(010) 88540776

发行传真：(010) 88540755　　发行业务：(010) 88540717

作者简介

刘映国，男，1964年5月出生，籍贯山西平陆。1982年9月入伍，先后就读于解放军测绘学院、国防大学，获工学学士与军事学硕士学位，中国国防科技信息中心研究员，硕士生导师，历任工程师、干事、研究室副主任、主任等职。长期从事武器装备与军事技术发展跟踪研究，牵头完成航天技术发展与装备建设领域重点科研项目60余项，获国家航天基金奖、军队科技进步一等奖2项、二等奖4项、三等奖2项，2次荣立三等功，多次获嘉奖。先后出版专著5部，发表学术论文40余篇，培养硕士研究生10名。

序

信息技术作为武器装备的力量倍增器，在现代战争中的地位与作用愈加凸显。与此同时，针对信息与信息系统固有脆弱性的网络攻击，已成为当前克敌制胜的一种新手段，确保武器装备信息系统安全势在必行。网络安全试验鉴定是武器装备履行使命任务的重要保证，在全寿命管理中发挥着不可或缺的作用。加强和推进网络安全试验鉴定是一项复杂的系统工程，既要有相应的政策法规作保障，又要深入研究网络安全试验技术、标准规范，以及靶场建设与人才培养等。

《美军网络安全试验鉴定》采用追根溯源的研究方法，系统分析了美国联邦政府对信息系统安全的具体要求，国防部开展网络安全试验鉴定政策演进，指标体系构建与试验流程规范，以及网络试验靶场建设最新进展，高端人才培养面临的挑战与对策措施等内容。该书以美军国防采办系统中的试验鉴定活动为对象，梳理了与网络安全试验鉴定直接相关的大量文献资料，深入研究了这些文献的内在逻辑关系及其在武器装备建设中具有的法律效力，并归纳总结了美军开展网络安全试验鉴定的主要意图与基本做法。美军认为，网络安全威胁已成为武器装备完成使命任务面临的巨大风险，特别是随着潜在对手网络攻击技术能力的不断增强，美军面临网络安全威胁的形势越来越严峻。因此，美军强调不仅要对在研武器系统进行网络安全试验鉴定，而且要对已部署装备进行网络安全风险评估，并通过年度部队训练演习对作战部队所有信息系统的脆弱性进行评估与修复。从近年来美军网络安全试验活动开展情况看，其在网络靶场建设、人才队伍培养、技

术研发、能力构建等方面已取得较大进展，正在为打赢一场网络空间战争积极储备力量。

网络安全试验鉴定是武器装备信息化建设的必然要求，反映了信息化时代装备发展的特点与规律。该书以新时代国家安全观为指导，以建设世界军事强国装备体系为目标，分析研究了网络安全试验鉴定的内容要求与基本流程，具有较强的探索性与前瞻引领作用。该书使用文献资料新颖丰富、翔实客观；内容全面系统，结构合理、逻辑性较强；既介绍了信息系统风险管理框架的概念与实施步骤，又描述了网络安全试验鉴定的具体内容；涉及专业面广，信息量大。相信本书对读者把握装备试验鉴定发展动向，研究谋划网络安全试验鉴定工作，推动试验鉴定法规制定、网络靶场建设与网络安全试验人才培养等将发挥积极的促进作用。

戴云辰

2018.3.26

前 言

近年来，美军发布大量网络安全（Cybersecurity）和网络安全试验鉴定的政策规定与工作指导文件，全面推进网络安全试验鉴定在国防采办系统中的应用，并对已部署武器系统通过作战演习进行网络安全评估。美军对网络安全脆弱性的敏感，既缘于其高度信息化的武器系统，又与其长期处于高技术局部战争实践直接相关。美军率先提出并全力推进网络安全概念在整个国防系统的广泛使用，旨在为新的战争形态储备力量，并为争夺新的军事优势聚集能量。网络安全试验鉴定是信息化武器装备规避网络空间威胁，打赢未来信息化战争不可或缺的一个重要环节。全面实施网络安全试验鉴定，美军所谋求的就是确保武器装备能够有效履行其使命任务，并有效抵御潜在对手可能发起的网络攻击，从而在战争全域赢得主动权。

洞察与把握美军在军事作战与装备建设领域的主要动向，是各国谋划军队建设与装备发展的重要基础。同样，学习借鉴先进技术国家军队建设基本经验与主要做法，对深化高技术条件下军队建设与装备发展规律认识，推进军队结构与规模编成改革有着积极的促进作用。为准确把控网络安全试验鉴定发展走向，作者搜集整理了60多份与网络安全试验鉴定相关的原始文献，对美军开展网络安全试验鉴定涉及到的法规依据、标准规范、试验指标，

以及网络靶场与人员队伍建设等内容进行了深入的分析研究和归纳总结。在此基础上，作者搜集整理了近3年来美军对在研武器系统实施网络安全试验鉴定，通过部队训练演习对已部署装备进行网络安全评估等情况，以及美军为提高网络安全试验鉴定能力而采取的各项战略措施。总的来看，美军强化网络安全试验鉴定是建立在对网络空间威胁规律深刻认识基础之上，有着全面制胜未来网络攻防对抗作战的针对性与目的性，应引起我们的高度重视与深入研究。

本书内容包含七章和附录部分。第一章着重介绍了美国《联邦信息安全管理法案》的演变，信息系统风险管理框架实施步骤与制定发布的相应标准规范等；第二章深入研究了美军试验鉴定管理体制，联邦信息安全管理法案在国防部系统的转化应用，以及信息系统风险管理框架成果作为网络安全试验鉴定输入并发挥的作用；第三章系统梳理了美军网络安全试验鉴定的六个阶段，每个阶段需要完成的主要工作与目标，以及各个阶段的输入与输出；第四章和第五章按照美军两个试验鉴定基本类型分别总结了各类试验活动组织实施过程与相应的网络安全试验指标体系，以及在《试验鉴定主计划》中编写网络安全试验内容的规范要求；第六章和第七章通过分析大量美国国防部相关机构年度报告，归纳总结了美军网络安全试验靶场与重要设施建设、人才队伍建设、试验技术研发等最新情况。此外，附录部分列举了两个典型系统实施网络安全风险管理框架的实例，以及网络安全试验鉴定常用缩略语。本书厘清了信息系统风险管理的政策演变，网络安全风险管理框架与试验鉴定的相互关系，美军装备试验鉴定相关知识，网络安全试验鉴定的地位作用与未来发展趋势。相信本书能够为读者进一步深入研究美军装备试验鉴定及网络安全相关问题，提供线索、参考与信息源。

本书在研究撰写过程中得到石根柱、李杏军、杨俊岭、欧渊等专家的大力支持，参阅了曹金霞、任惠民、郑晓娜等同志的部分研究成果，在此一并表示衷心感谢！显然，作者的专业背景与学识水平，都在一定程度上制约了对“网络安全试验鉴定”的理解和把握。尽管在有限时间内进行了刻苦钻研，但仍有大量问题是囫囵吞枣。作者对这一领域的研究刚起步，仍有不少问题需要深钻细研，书中不足之处，恳请专家、学者不吝指教。

作者

目 录

第一章　美国政府网络安全管理政策与演进

随着信息技术的快速发展及广泛应用，“互联网”（Internet）这一20世纪最伟大发明，已经将人类社会带入信息化时代。今天，“大数据”“云计算”“移动互联”等这些新概念与新技术，正在彻底改变着人们生产、生活、学习和工作的方式，进而不断重塑着经济社会发展的新模式。网络伴随着我们的日常生活，我们一刻也离不开网络。同时，网络的快速漫延使网络安全的概念不断变化，其内涵不断深化，外延也持续扩展。早期的网络安全主要包括物理安全、运行安全、数据安全等方面。当前，网络安全演变为更加广义的概念范畴，进入到整个网络空间（Cyberspace），其重点包括了信息系统安全、信息内容安全、运行环境安全、应用手段安全等多方面。近年来，网络空间安全事件频发，造成的危害与损失难以估量。有些事件造成的危害已明确显现，有些潜在而未爆发的事件，将可能会给一个国家的安全态势或部门的长远利益带来不可承受的巨大损失。我们生活在互联互通的网络空间，网络安全成为各国政府维护国家安全利益的重要领域。美国政府最早启动研究与发展网络安全管理政策，推动着网络安全攻防手段与技术发展，不仅加强了联邦政府机构信息系统的安全管理，而且促进了美军武器系统网络安全体系建设与发展。

第一节　美国《联邦信息安全管理法案》概述

美国作为互联网的发源地，对于网络的使用和安全的理解都要领先于其他国家，对互联网安全领域的立法工作也进行了较早的探索。起初，美国政府主要是针对单个计算机系统制定相关安全管理法规政策。随着网络的普及和网络安全事件的大量爆发，美国政府针对联邦机构的网络信息系统安全，开始制定并实施相关政策法案，并面向当前网络空间威胁制定安全标准与技术规范。

一、《联邦信息安全管理法案》演进

在美国尝试针对互联网进行立法管制的初期，立法多见于不同的专业领域，没有进行一般性的统一规划。同时，通过对这一时期美国政府立法的分析，普遍认为美国的网络安全最初阶段是为保护网络本身的正常运行与信息的安全传递，表述为以系统的安全为主。例如，美国政府早在 1987 年就发布了《计算机安全法案》（Computer Security Act of 1987），旨在确保计算机系统的正常运行与安全维护。这一法案被 2002 年发布的《2002 联邦信息安全管理法案》（Federal Information Security Management Act of 2002）替代。

2002 年 12 月 17 日，美国政府发布实施《2002 联邦信息安全管理法案》，这是 2002 年颁布的《2002 电子政务法案》（E-Government Act of 2002）中的第三章。该法案强调，信息安全对美国经济和国家安全十分重要，要求各联邦机构制定、记录和实施广泛的信息安全计划，确保支撑联邦机构及资产运转的信息与信息系统安全。其核心在于强化联邦政府对“网络安全”（Cybersecurity）的高度重视，并有效利用“基于风险管理政策，

提高安全费效比”。

为了推进《2002 联邦信息安全管理法案》的有效实施，美国国会对政府各联邦机构、白宫管理与预算办公室[①]和国家标准与技术研究院[②]，明确规定了在信息系统安全管理方面的具体职责与任务。其中，要求政府各联邦机构信息安全项目负责官员、机构的首席信息官和监察长，要对本机构的信息安全项目进行年度审查，并将审查结果向预算和管理办公室进行报告。预算与管理办公室根据各联邦机构提供的年度审查数据，对其履行职责情况进行监督，并为每年向国会提交联邦机构执行《2002 联邦信息安全管理法案》情况报告做准备。如 2008 财年，美国政府用于信息技术总投资约为 680 亿美元，其中，各联邦机构用于信息安全的费用达 62 亿美元，约占信息技术总经费的 9.2%。这些经费主要用于增强信息安全措施，为信息与信息系统提供安全保护，避免未经授权访问、使用、泄露、中断、篡改与损坏信息系统，确保所提供信息的可信性、完整性与可利用性。

国会赋予国家标准与技术研究院落实《2002 联邦信息安全管

① **白宫管理与预算办公室**：白宫管理与预算办公室（The Office of Management and Budget，OMB）是美国总统最大的一个执行办公室，其主要职能是为总统制定预算，但也评测各机构项目的质量、政策与规程，以确定其是否与总统的政策相一致，并协调跨部门间的政策倡议。该机构于 1970 年尼克松政策时期组建，并在 1990 年代由管理人员与预算人员重新组合而成，并在资源管理办公室对每个既定项目进行审查。白宫管理与预算办公室为总统向国会提供预算做准备，并对政府各分支执行机构进行监管。该机构还对政府采办、经费管理、信息与监管政策进行监督，其主要作用是帮助政府改进管理，并制定更好的协调机制，以减少公众不必要的负担。

② **国家标准与技术研究院**：美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务，在国际上享有很高的声誉。NIST 成立于 1901 年，原名美国国家标准局（NBS），1988 年 8 月，经美国总统批准改为美国国家标准与技术研究院（NIST）。NIST 下设 4 个研究所:国家计量研究所、国家工程研究所、材料科学和工程研究所、计算机科学技术研究所。所下设中心，中心下分组，组下设实验室。其中，计算机科学技术研究所负责发展联邦信息处理标准，参与发展商用 ADP 标准，开展关于自动数据处理、计算机及有关系统的研究工作。在制定联邦自动数据处理政策方面向白宫管理和预算办公室，以及国会总审计局提供科学和技术咨询。在计算机科学和技术方面向政府其他机构提供咨询和技术帮助。为完成各项具体任务，保持计算机科学和技术的能力，该所设有程序科学与技术和计算机两个中心。