美国网络安全漏洞披露管理情况研究

政务 (https://www.secrss.com/articles?tag=政务) · 信息安全与通信保密杂志社 (https://www.secrss.com/articles?author=信息安全与通信保密杂志社) · 2024-09-10

以点带面透视美国网络安全漏洞披露管理的体系化和多元化情况，对完善我国漏洞管理机制具有一定借鉴意义。

摘 要：网络安全漏洞披露是有效缓解攻防不平衡态势和降低网络安全风险的重要手段，美国在网络安全漏洞披露管理方面拥有一套行之有效的机制。为此，聚焦美国联邦政府互联网信息系统和国防部信息网络，分析其网络安全漏洞披露管理情况。首先，概述美国网络安全漏洞管理战略法规，了解其网络安全漏洞披露管理的战略布局和体系计划；其次，梳理国防部信息网络的漏洞管理依据和漏洞管理流程，分析以漏洞披露计划为代表的主要漏洞管理举措；最后，多角度分析联邦互联网系统漏洞披露的相关实践。以点带面透视美国网络安全漏洞披露管理的体系化和多元化情况，对完善我国漏洞管理机制具有一定借鉴意义。

内容目录：

0 引 言

1 美国漏洞管理重点战略法规

2 美国DoDIN漏洞管理的基本情况

2.1 美国国防部漏洞管理依据

2.2 美国国防部漏洞管理流程

2.3 美国国防部漏洞披露计划

3 联邦互联网信息系统漏洞披露管理的基本情况

3.1 约束性操作指令明确漏洞披露策略

3.2 联邦漏洞披露框架标准化漏洞披露流程

3.3 利用漏洞披露平台掌握潜在漏洞

3.4 漏洞指南标准化漏洞响应流程

3.5 特定漏洞紧急指令指导漏洞缓解

4 结 语

0 引 言

近年来，利用网络安全漏洞实施的网络攻击事件在全球范围内频发，给各国网络空间安全带来了不同程度的危害。漏洞管理作为识别、评估、披露、修复和减弱计算机系统中安全漏洞的过程，是管理信息技术（Information Technology，IT）环境中网络安全的关键部分和有效手段，对保护关键基础设施，维护国家网络安全具有重要实际意义。漏洞披露是指安全研究人员、IT安全团队、开发人员等将计算机软件或硬件中的漏洞信息通过公开渠道告知公众的过程，IT产品供应商和安全漏洞发现者通过该过程协同工作，寻找降低安全漏洞风险的解决方案。

1 美国漏洞管理重点战略法规

美国漏洞管理战略法规从国家战略政策到法规行政令，再到条令指南，覆盖全面。其中，关于漏洞披露的管理政策遵循《国家网络战略》《国家网络安全战略》等战略法规中有关促进和使用漏洞披露的总体布局，以及法规行政令的具体要求和条令指南等实施细则，美国漏洞管理重点战略法规如表1所示。

表1 美国漏洞管理重点战略法规

类目	名称
国家战略政策	《国家网络战略》
	《国家网络安全战略》
	《改进漏洞识别、管理和补救的备忘录》M-20-32
法规及行政令	《漏洞评估章程》
	《国务院黑客法案》H.R.328
	《公私网络安全合作法案》H.R.6735
	《网络漏洞披露报告法案》H.R.3202
	《国土安全部漏洞法案》S.1281
	《网络安全漏洞修补法案》H.R.2980
	《关于加强联邦网络和关键基础设施网络安全的行政令》E.O.13800
	《改善国家网络安全的行政令》E.O.14028
条令指令指南	《国防部漏洞管理指令》DoDI 8531.01
	《制定并发布漏洞披露政策》《降低已知被利用漏洞的重大风险》等系列约束性操作指令
	《网络安全事件和漏洞响应手册》
	《对联邦漏洞披露指南的建议》

战略政策方面，2018年9月，美国《国家网络战略》发布，明确“促进和使用协同漏洞披露、众包测试和其他创新性评估，以提高利用或攻击前的弹性”，从而“推进全生命周期网络安全”；2023年，《国家网络安全战略》指出，“为进一步鼓励采用安全软件开发实践，政府将鼓励在所有技术类型和行业中进行协调的漏洞披露”。

法规行政令方面，2020年9月，美国国防系统漏洞管理的主要指导性文件《国防部漏洞管理指令》（DoDI 8531.01）发布，范围覆盖管理和响应国防部信息网络（Department of Defense Information Networks，DoDIN）中所有软件、固件和硬件中发现的漏洞，明确用高效的漏洞评估技术、过程和功能支持国防部所有系统，满足《漏洞评估章程》（*Vulnerabilities Equities Process*，VEP）的相关要求，并确保提交新发现的未公开漏洞的效率，促进和保障漏洞披露。2021年5月，《改善国家网络安全的行政令》（E.O.14028）发布，强调了联邦政府应对网络安全漏洞和事件的流程标准化，确保对网络安全事件进行更加协调和集中的分类。

条令指令和指南方面，网络安全与基础设施安全局（Cybersecurity Infrastructure Security Agency，CISA）自成立以来发布了《制定并发布漏洞披露政策》《降低已知被利用漏洞的重大风险》等多份与漏洞管理相关的约束性操作指令，分别从漏洞披露、漏洞识别和漏洞跟踪等方面对联邦机构的漏

洞管理做出了明确要求。2021年11月，CISA又发布《网络安全事件和漏洞响应手册》，为联邦机构应对影响网络的漏洞和事件提供了一套标准程序。此外，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）在2023年5月发布《对联邦漏洞披露指南的建议》，就建立联邦漏洞披露框架、正确处理漏洞报告及沟通漏洞的缓解和/或修复提出了指导性建议，可供美国政府建立和维护统一的漏洞披露管理流程。

2 美国DoDIN漏洞管理的基本情况

DoDIN涵盖美国国防部所有网络空间，包括机密和非机密全球网络（如NIPRNET、SIPRNET、全球联合情报通信系统等），以及国防部智能手机、射频识别标签、工业控制系统、独立实验室网络和平台信息技术等。国防信息系统局等机构在《国防部漏洞管理指令》（DoDI 8531.01）要求下，按照特定流程及出台的系列举措开展漏洞管理。

2.1 美国国防部漏洞管理依据

美国国防部层面遵循《国防部漏洞管理指令》（DoDI 8531.01）实施漏洞管理，指令适用范围包括国防部长办公室组成部门、军事部门、参谋长联席会议主席办公室、作战指挥部、国防部总监察长办公室、国防机构和国防部内的所有其他组织实体。指令特点如下：

一是明确了美国国防部漏洞管理的目标。提供国防部漏洞管理流程，制定相关策略、分配责任，并对DoDIN中的所有软件、固件和硬件中的漏洞做出响应；建立基于联邦和国防部标准的统一的国防部部门级网络安全漏洞管理程序；为国防部漏洞披露计划（Vulnerability Disclosure Plan，VDP）制定策略并为其分配责任；根据美国政府的漏洞公平裁决政策和流程，制定策略、分配责任，并为国防部参与VEP提供程序指引。

二是美国国防部各部门协同进行漏洞管理。国防部的漏洞管理机构包括国防信息系统局、国家安全局、网络司令部、DoDIN联合部队总部、中央情报局、空军、NIST、国防部网络犯罪中心和国家安全委员会等，各部门各有职能侧重。该指令详细、清晰地赋予了国防部各相关部门漏洞管理的领导职责。

2.2 美国国防部漏洞管理流程

美国国防部漏洞管理流程包括漏洞识别、漏洞分析、分析报告、补救和缓解、验证和检查，如图1所示。一是漏洞识别，包括漏洞扫描、渗透测试、安全控制评估、历史文件、协同漏洞披露和VEP；二是漏洞分析，包括影响分析和优先级分析；三是分析报告，指国防部各部门起草和生成漏洞分析报告；四是补救和缓解漏洞，包括确定补救或缓解方法，考虑资产价值和风险暴露等因素，评估补丁有效性、监控合规性、补救及缓解措施等，按照美国国防部安全技术实施指南、国家安全局安全实施和缓解指南及NIST缓解指南，对软件、固件和硬件进行安全配置等；五是验证和检查，包括核实“补救和缓解”方法的效率，确保漏洞已被修复或减轻，监视已修复或减轻的系统、子系统或系统组件，以发现更多相互依赖的漏洞，持续监测受影响的系统。将日志存储在中央存储库或安全信息和事件管理平台中，遵循国防部信息安全持续监控计划，以满足联邦信息安全现代化法案的持续监控要求。

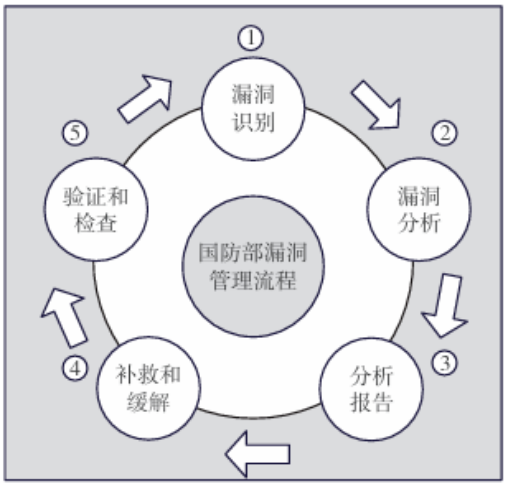

图1 美国国防部漏洞管理流程

2.3 美国国防部漏洞披露计划

美国国防部在漏洞管理方面有诸多举措，如国家安全局针对美国国家安全系统（National Security System，NSS）、美国国防工业基地和DoDIN发布漏洞指南并披露国家行为体的漏洞行为，缓解和避免漏洞利用风险等，而更具创新成效的披露举措是国防部漏洞披露计划（Department of Defense Vulnerability Disclosure Program，DoD-VDP）。

DoD-VDP于2016年建立，其源自“破解五角大楼”漏洞赏金试点计划，旨在通过加强DoDIN的安全性，为进一步实施网络空间深度防御策略提供保障。DoD-VDP建立了一个由国防部网络犯罪中心、美国网络司令部、DoDIN联合部队总部及HackerOne众包白帽黑客等组成的生态社区，通过HackerOne等众测平台开展漏洞赏金众测行动，发起多项漏洞赏金计划，发现更多有效漏洞，再由VDP网络分析师对报告中的漏洞进行验证、分类和处理缓解。

2021年1月，DoD-VDP范围正式从面向公众的网站扩展到所有可公开访问的国防部信息系统，通过与支持DoDIN的众包网络安全研究人员互动，扩大了对国防部网络攻击面的保护。截至2023年2月，美国国防部VDP已收到超过 45 000个漏洞，其中6 346个已成功缓解，近60%的漏洞被验证为可操作的。VDP漏洞逐财年严重程度报告如图2所示，显示了与黑客合作降低风险的巨大价值。

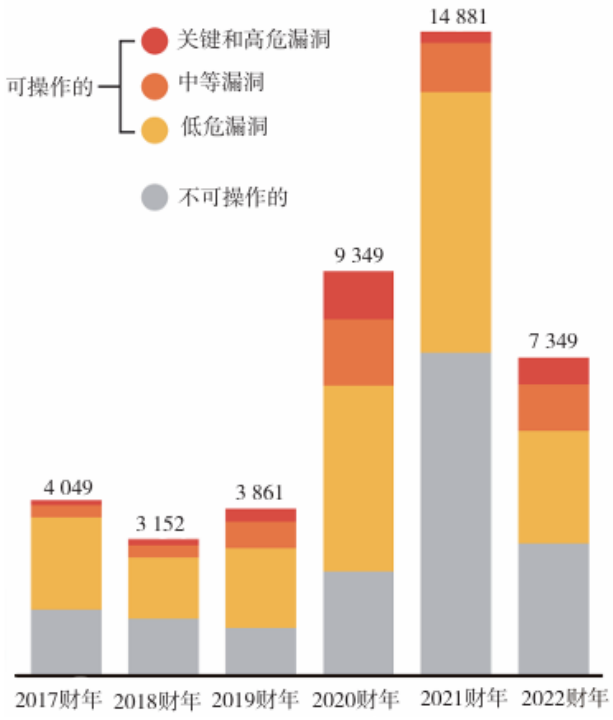

图2 VDP漏洞逐财年严重程度报告

（资料来源：美国国防部网络犯罪中心《2022 年度漏洞披露报告》）

DoD-VDP由3个方面组成：一是为开展众测活动提供明确指导方针和政策；二是保护白帽安全研究人员所报告问题的安全承诺，为其提供法律豁免；三是以合适的方式验证、筛选和修复漏洞的内部流程。自2018年开始，漏洞报告管理网络系统正式上线，可自动化、跟踪和处理所有报告，有效提高了国防部漏洞披露效率。

DoD-VDP有5个方面的能力：一是通过使用协同漏洞披露、众包测试和风险评估来提高全生命周期的网络安全，从而在漏洞被利用之前提高网络弹性；二是加强国防部与计算机安全研究人员的合作，建立积极的反馈循环，通过快速发现和修复漏洞来提高国防部网络的安全性；三是缩短发现漏洞、通知系统所有者和成功缓解漏洞之间的时间；四是为漏洞发现者向国防部报告提供开放渠道和合法安全港；五是通过提高国防部网络空间资产的弹性，促进国防战略行动路径——“建立一支更具杀伤力的力量”。

DoD-VDP有4个方面的优势：一是广泛利用大量白帽黑客的网络安全力量，深度防御7 349 DoDIN；二是通过发现网络中已存在的漏洞来减少攻击面，免于毁灭性网络攻击；三是在现有流程的基础上，依托国防部已有资源，实现近乎零成本的漏洞披露；四是实现对手模拟，白帽黑客使用相同的战术、技术和程序，相当于一支训练有素、装备精良的部队。VDP自实施以来，保障了2020年美国大选期间的网络安全，解决了针对DoDIN的关键和高危漏洞，并启动了一项为期12个月的国防工业基地漏洞披露试点计划，允许黑客在线报告 “几十家”国防工业基地公司运营系统中的漏洞。根据VDP 2022年度报告，国防工业基地漏洞披露试点计划共节省了6 140万美元的成本。

3 联邦互联网信息系统漏洞披露管理的基本情况

美国联邦政府民事机构漏洞管理工作由CISA负责，其在面向互联网的联邦信息系统漏洞管理方面有诸多举措，包括发布系列约束性操作指令、建立漏洞披露框架和漏洞披露平台、发布已知漏洞利用目录和紧急指令，以及漏洞规范化指南等，体现了其漏洞披露过程的逐渐规范化、智能化和公众化的趋向。

3.1 约束性操作指令明确漏洞披露策略

美国联邦机构正逐步扩大部署可访问互联网系统及相连接的复杂系统，但由于发现漏洞和利用漏洞之间的平均时间正在缩短，联邦政府认为必须继续采取快速修复漏洞等措施减少整体网络攻击面，并尽快将未授权访问联邦信息系统的风险降至最低。

CISA发布了系列约束性操作指令规范联邦漏洞管理。例如，2019年1月，CISA发布《互联网可访问系统的漏洞修复要求》的约束性操作指令（BOD 19-02），通过提高联邦层面对高危漏洞和关键漏洞的补救要求，进一步减少对联邦机构信息系统的攻击面和风险。2020年9月2日，CISA发布《制定并发布漏洞披露政策》的约束性操作指令（BOD-20-01），旨在使2020年成为 “漏洞管理年”，特别关注公众向政府部门披露漏洞的便利性问题，要求各联邦民事行政机构（Federal Civilian Executive Branch，FCEB）为其互联网可访问系统制定和发布VDP，并建立服务和维护流程以支持VDP，对漏洞披露策略、漏洞处理过程等提出了要求。随后发布的约束性操作指令BOD 22-1和约束性操作指令BOD 23-1也都从不同方面规范指导着联邦机构的漏洞管理。

3.2 联邦漏洞披露框架标准化漏洞披露流程

2023年5月，NIST发布了《对联邦漏洞披露指南的建议》（NIST SP 800-216），基于《ISO/IEC 29147：2018信息技术 安全技术 漏洞披露》《ISO/IEC 30111：2019信息技术 安全技术 漏洞处理流程》标准，专门为联邦政府建立了一个统一、灵活的漏洞披露框架，用于制定漏洞披露政策和实施程序，以报告、评估和管理联邦政府系统的漏洞披露。高级联邦漏洞披露框架和信息流如图3所示，主要政府参与实体是联邦协调机构（Federal Coordinate Branch，FCB）和漏洞披露项目办公室（Vulnerabi、公众和外部协调者。报告者是指向政府机构提交源漏洞报告的政府内外部实体；FCB是一组合作成员，共同提供灵活、高水平的机构间漏洞披露协调，政府通过FCB进行漏洞跟踪并提出漏洞咨询意见；VDPO是负责管理漏洞披露计划信息技术的办公室，负责与其他行为者协调，识别、解决和发布漏洞咨询报告；公众是指可能受到特定漏洞影响或需要针对特定漏洞采取行动的对象；外部协调者是指不属于FCB或VDPO的、接收源漏洞报告的任何漏洞披露实体。

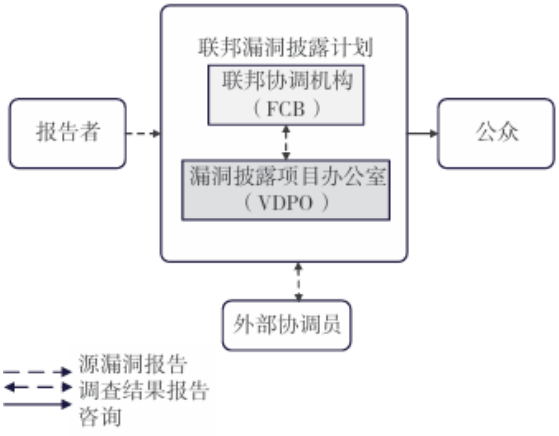

图3 高级联邦漏洞披露框架和信息流

3.3 利用漏洞披露平台掌握潜在漏洞

CISA网络质量服务管理办公室（Quality Services Management Office，QSMO）建立了面向联邦机公众构的VDP，该平台是一个软件即服务应用程序，由网络安全企业Bugcrowd和EnDyna为联邦互联网系统漏洞披露提供共享服务，如图4所示。该平台为联邦机构提供了一个统一的在线管理网站，使安全研究人员和公众能够在机构网站中发现其漏洞披露政策范围内的系统漏洞并提交报告以供各联邦机构分析。

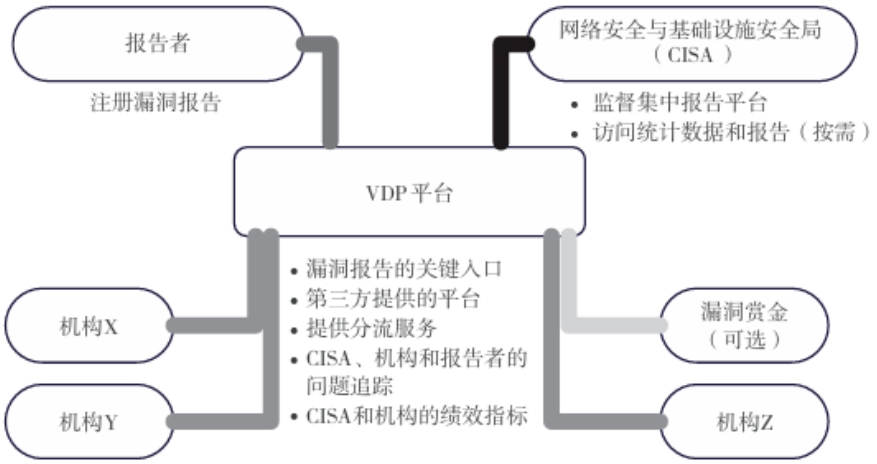

图4 CISA漏洞披露平台概念

该平台有4个方面的参与者：漏洞报告者、平台服务提供商、各联邦机构和CISA。漏洞报告者通过该平台报告联邦系统漏洞；平台服务提供商对提交的漏洞报告进行筛选和初步分类，验证合法性；CISA虽不主动参与具体漏洞补救过程，但保持对披露活动的监督，并访问所有机构的汇总统计数据和

报告，已识别漏洞的修复仍将由对应机构负责，而不是由CISA或VDP平台服务提供商负责。

该平台有两个方面的优势：一是统一集中管理，提高分析、解决和传达已披露漏洞的能力。联邦政府机构利用该平台作为研究人员披露、接收、分类和查找漏洞的主要入口，简化了与安全研究社区的协调方式，事件报告人可使用统一的网站来提交调查结果，提高整个联邦机构互联网可访问系统的安全性和协同披露。二是鼓励公私协作与信息共享，显著节省政府成本。该平台通过允许研究人员提交漏洞报告来鼓励公私部门间的协作和信息共享，拓宽政府机构了解和解决未知漏洞的渠道；对已识别的漏洞进行报告和分类，各机构无须开发独立系统报告和分类已识别漏洞，大幅提升机构专注处理漏洞的效率。CISA预测，通过利用QSMO的共享服务方法，将在政府范围内节省超过1 000万美元的成本。

3.4 漏洞指南标准化漏洞响应流程

CISA于2021年11月发布了《联邦政府网络安全事件与漏洞响应手册》，为FCEB提供了一套标准流程，用于识别、协调、补救、恢复和跟踪影响FCEB系统、数据和网络的事件和漏洞。该手册规范了政府机构应对紧急和高危漏洞时应遵循的流程，包括识别、评估、修复和报告漏洞4个阶段：一是识别阶段，通过监控威胁流和信息资源来主动识别被利用漏洞；二 是评估阶段，确定漏洞并评估底层软硬件重要性；三是修复阶段，及时修复系统或环境中存在的漏洞；四是报告和通知阶段，共享漏洞利用信息可帮助联邦政府机构防御者掌握亟须修复的漏洞。

3.5 特定漏洞紧急指令指导漏洞缓解

CISA会不定时发布漏洞紧急指令，要求联邦机构缓解特定漏洞。例如，CISA发布紧急指令ED 22-02，要求联邦机构评估其面向互联网的网络资产是否存在Apache Log4j漏洞，并立即修补这些系统或实施其他缓解措施。CISA建立了一个专门的Log4j网页，内容即CISA与联邦调查局、NSA、澳大利亚网络安全中心和加拿大网络安全中心等机构联合发布的网络安全建议，包含用于网络防御者的Log4j技术细节、缓解措施和资源，以及受影响设备和服务的GitHub软件。

4 结 语

漏洞已成为网络空间的重要战略资源，美国漏洞披露管理的发展实践预示着健全的漏洞披露体系和开放多元的漏洞披露计划，是快速掌握漏洞资源和实现漏洞缓解的制胜法宝。我国已初步建立漏洞管理体系，在漏洞法规出台、标准体系建立、漏洞运营管理等工作上取得了一定成效，应进一步借鉴成熟经验，建设规范有序、充满活力的漏洞收集和发布渠道，增强网络弹性，防范网络安全重大风险，保障国家网络安全。

引用格式：刘力平,尹晗,张玲,等.美国网络安全漏洞披露管理情况研究[J].信息安全与通信保密,2024(6):30-38.

作者简介 >>>

刘力平，女，硕士，工程师，主要研究方向为网络空间安全战略研究；

尹 晗，女，硕士，高级工程师，主要研究方向为网络空间安全战略研究；

张 玲，女，硕士，研究员，主要研究方向为网络空间安全战略研究；

罗 仙，女，硕士，高级工程师，主要研究方向为网络空间安全战略研究。

选自《信息安全与通信保密》2024年第6期（为便于排版，已省去原文参考文献）

政务 (https://www.secrss.com/articles?tag=政务)

军队军工 (https://www.secrss.com/articles?tag=军队军工)

漏洞管理 (https://www.secrss.com/articles?tag=漏洞管理)

相关资讯

“盐台风”登陆，美国政府窃听系统遭反窃听？ (https://www.secrss.com/articles/70946)

信息通信 (https://www.secrss.com/articles?tag=信息通信) · GoUpSec (https://www.secrss.com/articles?author=GoUpSec) · 10小时前

带路国家科威特卫生部被黑，致使国内多个医疗服务中断 (https://www.secrss.com/articles/70844)

医疗卫生 (https://www.secrss.com/articles?tag=医疗卫生) · 安全内参 (https://www.secrss.com/articles?author=安全内参) · 2024-09-30

瞄准国内政企！深度揭秘的勒索软件运营商Rast gang (https://www.secrss.com/articles/70601)

政务 (https://www.secrss.com/articles?tag=政务) · 奇安信威胁情报中心 (https://www.secrss.com/articles?author=奇安信威胁情报中心) · 2024-09-25