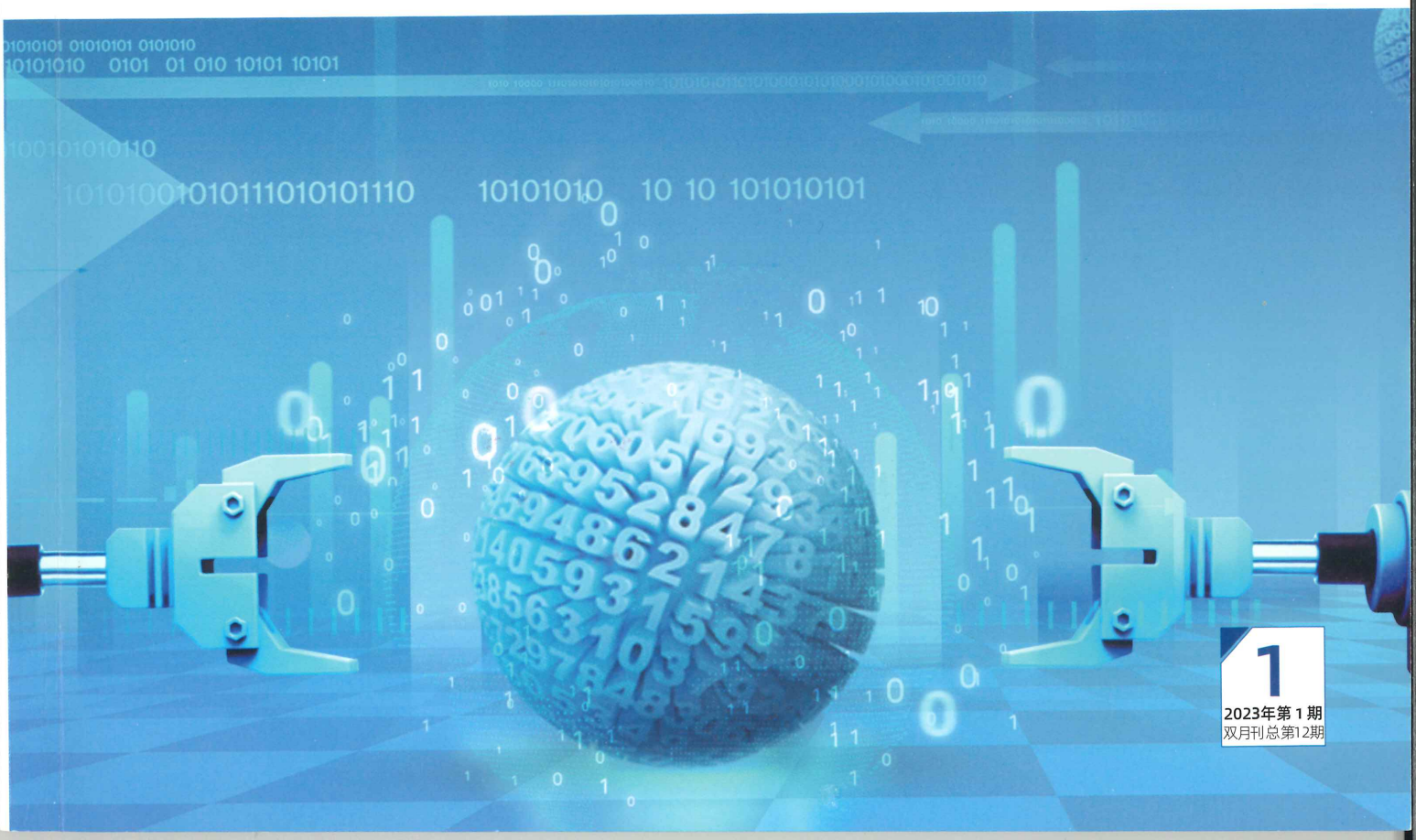
主管单位：工业和信息化部
主办单位：国家工业信息安全发展研究中心

ISSN 2097-1176
CN 10-1802/TP

工业信息安全

INDUSTRY INFORMATION SECURITY



CONTENTS

目 次

CONTENTS 目次

美国提升关键基础设施网联设备安全措施分析

杨婷[1]，左晓栋[2]

1. 中国软件评测中心，北京，100048

2. 中国科学技术大学公共事务学院、网络空间安全学院，安徽合肥，230026

摘要：本文总结分析了美国政府问责署（GAO）发布的《提升网络连接设备安全的举措》主要内容和联邦政府为此开展的相关行动，以及根据审查结果和发现，GAO 向美国能源、卫生与公众服务、国土安全、交通部门以及公共管理和预算办公室提出增强其基础设施中 IoT（物联网）和 OT（操作技术）网络安全的实施建议。最后，本文对我国关键信息基础设施相关网络安全措施提出了建议。

关键词：关键基础设施；物联网；运营技术；网络安全

Study on US Actions to Better Secure Internet-Connected Devices of Critical Infrastructure

Yang Ting[1], Zuo Xiaodong[2]

1. China Software Testing Center, Beijing, 100048

2. School of Public Affairs, and School of Cyber Space Security, University of Science and Technology of China, Hefei Anhui, 230026

Abstract: The paper reviewed Actions Needed to Better Secure Internet-Connected Devices, issued by US Government Accountability Office in Dec., 2022, which proposed 9 recommendations to Department of Energy, Departent of Health and Human Services, Department of Homeland Security, Department of Transportation and Office of Management and Budget. According to the analysis and the protection practices for cybersecurity of Internet of Things and Operational Technology in national critical infrastructure, it is suggested that enforcing cybersecurity inspection, coordinating national resources and strengthening cybersecurity capabilities will improve our national critical IT infrastructure security.

Keywords: Critical Infrastructure; Internet of Things; Operational Technology; Cybersecurity

---

基金项目：国家重点研发计划项目“重要数据分类、识别与安全评估技术”2022YFB3103200。

作者简介：杨婷，女，中国软件评测中心工程师，主要研究方向为网络安全、工业控制系统安全，E-mail: yangting@cstc.org.cn。

通讯作者：左晓栋，男，中国科学技术大学公共事务学院、网络空间安全学院教授，主要研究方向为网络空间治理，E-mail:xdzuo@ustc.edu.cn。

引言

当前，全球网络安全形势日趋复杂严峻，各国关键信息基础设施安全防护面临巨大挑战。过去，美国已经建立了完善的关键基础设施保护制度与管理体系[1]-[3]。2022 年 9 月，网络安全与基础设施安全局（CISA）发布了首个综合性战略规划《2023 年至 2025 年战略规划》，明确了未来 3 年美国网络和基础设施安全工作的方向，旨在降低美国关键基础设施的安全风险，增强弹性。

我国也高度重视关键信息基础设施安全保护工作。2017 年 6 月 1 日施行的《网络安全法》明确规定对关键信息基础设施实行重点保护。2021 年 9 月 1 日，《关键信息基础设施安全保护条例》正式施行。国家标准 GB/T39204-2022《信息安全技术 关键信息基础设施安全保护要求》将于 2023 年 5 月 1 日实施，其它多部配套国家标准正在研制中。

随着物联网等技术在重点行业的大量应用，国内外关键信息基础设施安全保护面临新的形势，其网络暴露面增大、脆弱点增多，有必要完善已有标准、进一步提升安全防护能力。美国在这方面率先开展了研究，美国政府问责署（GAO）于 2022 年 12 月发布的《提升网络连接设备安全的举措》（以下简称《报告》）显示，关键基础设施使用的物联网设备仍缺乏足够的安全防护，这在全球可能也是普遍现象。为此，GAO 提出了有关加强关键基础设施物联网设备安全的建议。《报告》提出的措施建议可供我国相关工作参考。（考虑到中美两国分别使用“关键信息基础设施”和“关键基础设施”，本文未作区分）。

1 美国 GAO 提升网联设备安全报告概述

传统上，美国的关键基础设施保护对象主要针对的是传统 IT（信息技术）系统和电子数据处理系统，随着时间的发展逐步将数据安全（含个人信息）、工业控制系统纳入其中[4]。这个过程是与技术演进以及外部威胁变化情况保持一致的。

近年来，美国政府意识到，随着关键基础设施中物联网技术的应用，针对联网设备和运营技术的网络威胁开始增多，正在成为国家安全的一项重大挑战，一批重大网络安全事件的发生都证明了国家关键基础设施面临的此类威胁呈上升趋势。如 COVID-19 疫情流行期间，针对健康医疗和基本服务的勒索软件攻击屡有发生。这些问题引起了 GAO 的关注。美国国会在《2020 年物联网网络安全提升法案》中便加入了 GAO 当时关于物联网（IoT）和运营技术（OT）网络安全调查的相关内容。

但经过几年的发展，物联网应用引发的这一问题并没有得到明显缓解。为此，2022 年 12 月，GAO 又一次发布报告《提升网络连接设备安全的举措》。《报告》指出，美国的 16 个关键基础设施行业要依靠网络连接设备和系统来提供基本服务，例如电力和健康医疗，但其正在面临日益严重的网络安全威胁，虽然被审查的三个行业（能源行业、健康医疗和公共卫生行业、交通行业）中主责联邦机构已将采取了一些控制措施，但却没有评估网络连接设备和系统对整体行业的风险。而如果没有全面的网络安全风险评估，运营者便不可能知道本行业还需要哪些进一步的网络安全保护措施。正是出于解决这类问题的初衷，GAO 基于审查发现提出了增强关键基础设施物联网设备安全的建议。

GAO 评估了被抽查联邦机构（保障物联网和运营技术网络安全的主责部门）所采取的各项行动和举措。首先，GAO 确定了被认为具有最大网络入侵风险的六个关键基础设施行业。然后，GAO 从中选择了三个广泛使用物联网和运营技术设备与系统的行业进行审查，即能源行业、健康医疗和公共卫生行业、交通行业。对于每一个行业，GAO 进行了相关文件分析、部

表 1　主责联邦机构采取的 IoT 或 OT 网络安全举措

行业（主责联邦机构）	IOT 或 OT 网络安全举措示例
能源（能源部）	（1）《OT 网络安全监控技术注意事项》：针对监控系统 OT 网络安全技术，提出了评估注意事项，如通过电网进行电力分配的系统。 （2）《OT 环境网络安全方法》：旨在提高能源行业对 OT 网络中异常行为威胁的检测，如配电网络。
健康医疗与公共卫生（卫生与公众服务部）	（1）《网络安全管理上市前指南》：针对医疗器械设计和开发，确定了制造商应考虑的网络安全相关问题，如诊断设备。 （2）《医疗器械上市后网络安全管理》：针对已上市和已售出医疗器械，提出了网络安全漏洞管理建议，如输液泵。
交通（国土安全和运输部）	（1）地面交通系统网络安全工具包：针对交通控制系统，提供网络风险管理工具和资源，如船舶机械控制系统。 （2）国土安全部运输安全管理局发布的《加强铁路网络安全指令》：规定了需要开展的各种行动，如进行网络安全漏洞评估、为高风险铁路制定网络安全事件响应计划等。

门官员访谈，以及将主责机构采取的行动与联邦要求进行了比较分析。

2 美国 GAO 的审查结果与发现

美国关键基础设施行业正常运行很大程度上依赖于电子系统，包括物联网（IoT）和运营技术（OT）设备与系统。这里，物联网通常是指允许各种“事物”进行网络连接和交互的技术与设备，遍布房屋建筑、交通运输设施或家庭等；运营技术是指与物理环境交互的可编程系统或设备，例如控制机器以调节和监控温度的楼宇自动化系统。

图 1　信息技术、物联网和运营技术互联关系图

为了帮助联邦机构和私营实体管理物联网和运营技术相关的网络安全风险，美国国土安全部（DHS）网络安全和基础设施安全局（CISA）会同美国国家标准与技术研究院（NIST）发布了实施指南，并提供了多种工具和资源。其中，CISA 发布实施了 IoT 安全指南、启动了专项计划、提供了关于物联网和运营技术设备漏洞的警示和建议，并建立了运营技术工作组；NIST 发布了多份关于物联网和运营技术的指导文件，建立了网络安全卓越中心，并建立了多个支撑工作组。此外，联邦采购监管委员会正在考虑更新《联邦采购条例》，以更好地管理物联网和运营技术的网络安全风险。

调查分析表明，能源、健康医疗和公共卫生、交通行业广泛使用了物联网和运营技术设备与系统。为了帮助这些行业提升安全防护能力，被抽查的主责联邦机构报告了其实施的各种网络安全举措。

审查结果表明，被抽查主责机构都没有为评估其工作的有效性而制定绩效考核标准，也没有进行物联网和运营技术网络安全风险评估。这两项活动都是增强网络安全防护能力的最佳做法。被抽查主责机构官员指出，仅依赖行业实体组织自愿提供的信息，难以评估政策法规、技术规范的有效性。然而，如果不对物联网和运营技术进行风险评估和有效性评价，那么旨在降低物联网和运营技术风险的各种举措是否成功实施，显然是未知数。

《2020 年物联网网络安全提升法案》规定，在 2022 年 12 月 4 日之后，如果物联网设备不符合 NIST 制定的标准，联邦机构将禁止进行采购或使用。根据法案要求，NIST 于 2021 年 6 月发布了一份指导文件草案，提出了相关要求，用以指导联邦机构、企业和行业接收和上报漏洞信息。该法案还要求美国公共管理和预算办公室（OMB）为联邦机构建立一个标准化流程，

以明确规定：只有在满足法案中规定的豁免条件时，联邦机构才可以不遵守禁止采购或使用不合规物联网设备的规定。

截至 2022 年 11 月 22 日，OMB 尚未制定这一强制实施流程。OMB 官员指出，豁免流程的制定需要与其他实体进行协调并收集相关数据。根据 OMB 提供的信息，豁免流程指南原计划于 2022 年 11 月发布，已经明显滞后。根据法案要求，从 2022 年 12 月开始，联邦机构将禁止使用不合规的物联网设备。因此，豁免程序的缺失，可能会导致各机构落实法案要求的不一致性。

3 美国已经制定发布的 IoT 和 OT 安全指南

《报告》梳理了美国已经制定发布的 IoT 和 OT 安全指南。

3.1 美国联邦政府制定的指南或开展的行动

（1）统一漏洞披露计划。该计划统筹发布产品和服务中最新发现的网络安全漏洞和修复措施，既包括 OT 中最新漏洞（如 ICS，工业控制系统），也包括 IoT 和传统 IT 漏洞。联邦政府官员指出，本计划同等对待和处理 IoT 漏洞和 IT 漏洞，并没有把他们进行区分。

（2）具有约束力的操作指令 [6]。指令要求联邦机构保护联邦机构的信息和系统的安全，包括 IoT 和 OT，免受已知或可疑安全威胁、漏洞或风险的影响。例如，2021 年 11 月，针对联邦企业具有重大风险的已知漏洞，包括 IoT 设备中的漏洞，《具有约束力的操作指令》22-01 建立了一个由 CISA 管理的目录，以及联邦机构修复目录中漏洞的要求。2022 年 10 月，CISA 发布了《具有约束力的操作指令》23-01，要求所有联邦民用执行机构维护和及时更新联网资产清单，并确定软件漏洞。

（3）ICS 联合工作组 [7]。2009 年，DHS 建立了 ICS 联合工作组，通过对 16 个关键基础设施行业，在联邦、州和当地政府、资产拥有者和运营者、零售商和其他相关方之间建立合作伙伴关系，降低美国 ICS 的网络风险。ICS 联合工作组还每两年举办一次研讨会，促进关键基础设施相关方学习掌握 ICS 中的关键网络安全问题、收集和交换网络安全观点。工作组每个季度会发布简讯，告知 ICS 安全研讨会安排、重大事件、培训、技术发展以及其他相关事项。

（4）网络监测平台。CISA 官员指出，CISA 管理的威胁检测与监控平台是为了帮助关键基础设施行业对关键 IT 和 OT 网络实现可视化运营，确定和抵御网络风险和事件。平台可以监测关键基础设施网络，以发现那些影响相关方的已知和未知恶意行为，并提供三方面安全增强措施：一是为行业实体和 CISA 提供过往和现在网络态势感知信息；二是帮助 CISA 跨行业分析网络安全事件，确定事件特征和发展趋势；三是为 CISA 提供运营分析，进而提醒保护大型关键基础设施社区和联邦资产。

（5）CISA 网络评估。CISA 提供了八种不同的网络评估工具，供公共和私营部门选择使用，如实体组织可能需要的风险和漏洞评估、结构设计评审等。CISA 提供这些评估并不是针对个别行业，而是服务于所有行业，当然也不是为 IoT 和 OT 而定制的。另外，CISA 一直在积极平衡有限的资源，提供上述服务项目。CISA 报告表明，2019 年财年到 2022 财年，在被审查的三个行业中开展了 79 项结构评审，而且收到了 154 项结构评审的开放申请。

（6）总统国家安全通信咨询委员会（NSTAC）[8]。NSTAC 由总统咨询委员会根据联邦咨询委员会法案领导，并由 DHS 负责日常运营。它针对政府如何落实管理政策或采取措施提高国家安全和通信应急能力，向总统执行办公室提供工业安全分析和提升建议。2021 年 5 月，在经历了一系列重大网络安全事件之后，白宫指派委员会就“2021 年和将来提升网络韧

性”开展多阶段研究，要求尤其要聚焦于 IT 和 OT 安全。

（7）联合网络防御协作（JCDC）。2021 年 8 月，JCDC 是由 CISA 联合公共和私营部门成立的一个合作组织，主要成员来自关键基础设施行业的工业合作伙伴。他主要是想推动关键基础设施领域开展跨部门的网络安全合作。2022 年 4 月，CISA 扩展了 JCDC 的范围，将 OT 纳入进来，尤其是包括那些具有 ICS 经验的公司。

3.2 NIST 制定的技术规范

近年来，NIST（美国国家标准技术研究院）先后制定发布了与 IoT 和 OT 有关的如下技术规范：

（1）NIST IR 8228《关于 IoT 网络安全和隐私风险管理的考虑》（2019 年 6 月）；

（2）NIST IR 8259《IoT 设备生厂商的基本网络安全活动》（2020 年 5 月）；

（3）NIST IR 8259A《IoT 设备网络安全能力核心基线》（2020 年 5 月）；

（4）NIST IR 8259B《IoT 非技术支持能力核心基线》（2021 年 8 月）；

（5）NIST SP800-213《联邦政府 IoT 设备网络安全指南：建立 IoT 设备设备网络要求》（2021 年 11 月）；

（6）NIST SP800-213A《联邦政府 IoT 设备网络安全指南：IoT 设备网络安全要求目录》（2021 年 11 月）；

（7）NIST IR 8425《消费者 IoT 产品核心基线保护轮廓》（2022 年 9 月）；

（8）NIST SP800-82《OT 安全指南》（修订 3 草案）（2022 年 4 月）。

3.3 美国联邦采购监管委员会拟采取的措施

美国联邦采购监管委员负责 FAR（联邦采购法）的修订和管理。国防采购监管委员会和民用机构采购委员会共同准备发布 FAR 的修订。2022 年 9 月，联邦采购监管委员会官员指出，委员会正在考虑根据 NIST IoT 网络安全指南和 OT 安全要求（根据 14028 号总统指令“增强国家网络安全”制定的）修订 FAR。同时，委员会也在考虑 FAR 其他网络安全方面的修改，包括 IoT 和 OT 设备网络安全风险相关要求。例如，FAR 案例 2018-017《特定远程通信和视频监控服务和设备禁令》、2019-009《与使用特定远程通信和视频监控服务和设备的企业签约禁令》[9][10]。这些文件要求，禁止从几个外国技术公司采购特定的远程通信和视频监控设备和服务，包括 IoT 和 OT。截止到 2022 年 9 月份，美国国防部、美国总务管理局和美国国家航空航天局正在处理 FAR 相关规则。

4 美国 GAO 的实施建议

根据审查结果和发现，美国 GAO 共提出了九项实施建议。其中，GAO 向被审查行业的主责机构提出了八项建议，包括能源部、卫生和公共服务部、国土安全部和运输部。GAO 建议各行业建立和使用考核指标对物联网和运营技术网络安全工作的有效性进行评价，并评估行业物联网和运营技术的网络安全风险。同时，GAO 向 OMB 提出了一项建议，要求尽快建立物联网网络安全豁免流程。

美国国土安全部和运输部同意这些建议，而能源部表示，要在与其他机构进一步协调之后，才能对这些建议做出回应。卫生与公众服务部既未同意也不反对这些建议，但提出了计划采取的行动。具体而言，卫生与公众服务部计划更新其行业计划，但也表示不会强迫私营部门实施该计划。GAO 也坦承，包括卫生与公众服务部在内的美国联邦机构与关键基础设施行业之间仅是一种自愿性质的关系，无法强制行业遵从，但其依然建议政府部门建立物联网和运营技术考核指标，以便为行业建立问责制、记录实际绩效和促进有效管理提供基础，并为相关决策提供反馈机制。

表 2　行动建议

受影响机构	实施建议	进展情况
能源部	建议一：能源部部长作为能源行业的行业风险管理机构（SRMA），应指导网络安全、能源安全和应急响应办公室主任根据《国家计划》制定行业计划，其中包括衡量其提高本行业 IoT 和 OT 环境网络安全所开展工作的有效性指标。	尚未采取满足建议的行动，或者相关行动尚在计划中。
能源部	建议二：能源部部长作为能源行业的 SRMA，应指导网络安全、能源安全和应急响应办公室主任将 IoT 和 OT 设备纳入部门网络环境的风险评估中。	尚未采取满足建议的行动，或者相关行动尚在计划中。
卫生与公众服务部	建议三：卫生与公众服务部部长作为健康医疗和公共卫生行业的 SRMA，应指导负责准备和应急响应的助理部长根据《国家计划》制定行业计划，其中包括衡量其提高本行业 IoT 和 OT 环境网络安全所开展工作的有效性指标。	尚未采取满足建议的行动，或者相关行动尚在计划中。
卫生与公众服务部	建议四：卫生与公众服务部部长作为健康医疗和公共卫生行业的 SRMA，应指导负责准备和应急响应的助理部长将 IoT 和 OT 设备纳入部门网络环境的风险评估中。	尚未采取满足建议的行动，或者相关行动尚在计划中。
国土安全部	建议五：国土安全部部长作为交通运输部门的联合 SRMA，应指导运输安全管理局局长和美国海岸警卫队司令与运输部情报、安全和应急响应办公室合作，根据《国家计划》制定行业计划，其中包括衡量其提高本行业 IoT 和 OT 环境网络安全所开展工作的有效性指标。	尚未采取满足建议的行动，或者相关行动尚在计划中。
国土安全部	建议六：国土安全部部长作为交通运输部门的联合 SRMA，应指导运输安全管理局局长和美国海岸警卫队司令与运输部情报、安全和应急响应办公室将 IoT 和 OT 设备纳入部门网络环境的风险评估中。	尚未采取满足建议的行动，或者相关行动尚在计划中。
运输部	建议七：运输部部长作为交通运输部门的联合 SRMA，应指导情报、安全和应急响应办公室主任与国土安全部运输安全管理局局长和美国海岸警卫队司令合作，根据《国家计划》制定行业计划，其中包括衡量其提高本行业 IoT 和 OT 环境网络安全所开展工作的有效性指标。	尚未采取满足建议的行动，或者相关行动尚在计划中。
运输部	建议八：运输部部长作为交通运输部门的联合 SRMA，应指导情报、安全和应急响应办公室主任与国土安全部运输安全管理局局长和美国海岸警卫队司令将 IoT 和 OT 设备纳入部门网络环境的风险评估中。	尚未采取满足建议的行动，或者相关行动尚在计划中。
管理和预算办公室	建议九：OMB 主任应根据《2020 年物联网网络安全提升法案》的要求，及时为相关机构的首席信息官（CIO）建立标准化流程，指导他们确定是否符合 IoT 网络安全的豁免条件。	尚未采取满足建议的行动，或者相关行动尚在计划中。

5 对我国关键信息基础设施网联设备安全保护的启示

我国大多数关键信息基础设施由国家管理，但总体网络安全防控能力尚比较薄弱，对新技术应用更缺乏安全风险防控措施[11][12]。因此，结合美国关键基础设施保护经验，特别是《报告》所反映的情况，我国关键信息基础设施保护工作可考虑从以下方面进行完善。

一是针对物联网应用出台专门管理要求和标准规范。目前，我国关键信息基础设施网络安全标准体系虽然已有布局，但正式发布的仅有一部，其他正在制定的标准还没有细化到 IoT 和 OT 技术，这与很多关键基础设施天然便采用工控协议、近年来大量部署智能化物联网设备的形势不相适应。鉴于物联网设备应用的高比例，建议将今后关键信息基础设施网络安全标准的编制重点适当向物联网设备倾斜。

二是面向高烈度网络安全攻击，提升实战对抗能力。经分析美国已经发布的 IoT 和 OT 技术文档，其显著特点是针对性强，往往是为了应对特定攻击手法。在编制之前，其已经对通过物联网设备入侵关键基础设施的手段进行了反复验证，例如对近年来肆虐的勒索病毒攻击进行了复盘，并以此为基础提出防范措施。持续至今的俄乌冲突也表明，物联网设备已经被攻防双方“盯上”，被推向了对抗一线。因此，当前在普适性地加强物联网安全的同时，还要专门研究攻击者通过物联网设备入侵关键信息基础设施的方法手段，从更激烈对抗角度提出应对方案。

三是落实网络安全和数据安全审查制度，增强供应链安全。美国发布《报告》的最终结论指向安全评估，认为美国联邦政府在此方面无所作为，这客观上反映出该领域技术方法和实践的空白。我国开展网络安全风险评估的历史

已有多年，近年来又实施了网络安全审查等制度建设，但物联网设备是目前审查的薄弱环节，建议针对关键信息基础设施运营者采购物联网设备明确专门的审查要点。

6 小结

本文分析了美国政府问责署（GAO）2022年12月发布《提升网络连接设备安全的举措》背景，跟踪介绍了美国联邦机构在增强IoT和OT网络安全方面的整体计划和已开展工作，总结了GAO对能源、健康医疗和公共卫生、交通三个行业进行审查的结果和发现，以及GAO对这三个行业和OMB提升其基础设施中IoT和OT网络安全的实施建议。结合美国GAO报告内容和我国关键信息基础设施保护实际，本文提出我国加强关键信息基础设施物联网安全的有关建议。

参考文献

[1] 张弛，崔占华．美国关键基础设施安全管理综述[J]. 信息安全研究，2017, 第3卷(8): 736-745.

[2] 左晓栋．国外关键信息基础设施安全监管概述[J]. 中国信息安全，2016, 第11期:52-53.

[3] 左晓栋．美国网络安全战略与政策二十年[M]. 电子工业出版社，2018年1月：546-553.

[4] US GAO, https://www.gao.gov/highrisk/ensuring-cybersecurity-nation.

[5] US GAO, https://www.gao.gov/products/gao-23-105327.

[6] US CISA, https://www.cisa.gov/binding-operational-directive-22-01.

[7] US CISA, https://www.cisa.gov/uscert/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

[8] US CISA, https://www.cisa.gov/about-presidents-nstac.

[9] https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-C/section-200.216.

[10] https://www.ecfr.gov/current/title-48/chapter-1/subchapter-H/part-52/subpart-52.2/section-52.204-25.

[11] 网络安全等级保护网（2022年8月18日），http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a81825680dbc18f0182f36c3d1c00d7.

[12] 中央网信办（2021年09月03日），http://www.cac.gov.cn/2021-09/01/c_1632086524390279.htm.