Circular From WOE
Date: 7 January 2021

美国海岸警卫队发布网络风险管理指南

针对所有贸易至美国的船舶的网络风险管理指南于 2021 年 1 月 1 日生效。指南 CVC-WI-027(1)具体细节可点击此处查看。

要点：

- 每个船旗国都在该指导范围内
- 严重缺陷被要求在 90 天内修复并进行外部审核，否则有被拘留的风险
- 轻微缺陷需在 90 天内进行内部审核，并在开航前修复
- 检查的范围只包括和船舶安全直接相关的网络系统
- 如果对船舶安全至关重要的系统发生故障时，检查人员/港口安全管理员会被委派调查该问题是否和网络相关。如果相关，将调查在故障发生前是否遵循了正确的程序
- 如果检察人员认定有理由采取进一步检查，并且收集到明确的证据证明船舶安全管理体系中的网络风险管理部分存在执行不力，则可能开具进一步的缺陷证明
- 该指南聚焦船舶安全和安保。环境保护也在检查的范围内，但文件中未强调

该指南将影响在美国贸易或运营的任何船旗国的船舶和海上设备。

美国海岸警卫队将检查船舶/海上设施的哪些方面？

理想情况下，他们会发现船舶在其安全管理体系中完全整合了网络风险管理，并有充足的文件证明这一点。然而他们的任务是寻找不良网络环境问题的证据，包括但不限于如下方面：

A. 不良网络环境(比如显示密码或登录名、默认登录或无登录名、一段时间不活动后没有自动登出、严重依赖 USB 并且插入 USB 前没有检测病毒）
B. 证据表明船舶的电脑上有恶意软件——弹出窗口/任何勒索软件
C. 有关于影响船上系统的异常网络活动/安全性问题的记录或投诉

D. 疑似来自船长/船员的伪造/钓鱼邮件

如果网络安全被发现有缺陷该怎么办？

如果有任何不良的迹象，检查员会进一步调查是否存在缺陷，但仅调查船舶安全操作或航行所需的系统，独立系统或不影响船舶安全运营或航行的其他系统不予检查。

船东须注意船上的八个关键系统: 压载控制、引擎及推进控制、舵机控制、货物管控、导航(ECDIS/GPS)、雷达、卫星以及 3G/4G/5G 通讯，以及船上福利系统。

最关键的是，如果海事检验员/港口国船舶安全检查员发现有缺陷处理不当、或者他们能够得出结论认为船舶因不再符合《SOLAS 公约》而不适航，船舶很可能被扣留。

检查人员将怎么处理缺陷？

当缺陷被发现或查明时，检查人员有三种选择:

1. 如果网络安全风险管理没有纳入海上安全管理系统，检查员可开出代码 30 的缺陷证明——导致扣船。
2. 如海事检查员清楚地知道船舶安全管理系统存在网络组件，但并没有遵从指导(作为网络环境不良的证据) ，检查员可开出代码 17 的缺陷证明——要求船舶离港前修正缺陷。
3. 如有证据显示船舶的网络安全已纳入其安全管理系统但严重违反了网络安全规定，海事检查员可开出代码 30 的缺陷证明——导致扣船。

船只可能会被扣留吗？

是的，请详见上文。简而言之，如果网络风险管理系统没有实施或未以允许的方式实施、又或者未能防止网络事故，那么船舶可能面临两种缺陷证明，代码 17——要求在到达下一个美国港口前对该缺陷进行补救，或者代码 30——将被扣船直到补救措施完成。

如果船舶有缺陷，应该怎么做？

如果有缺陷，船东无论如何都要在重新进入美国之前的 3 个月内对缺陷进行修复并进行外部审查。如果缺陷更多算是关于偶尔的失误，则船东必须在 90 天内进行内部检查，并在开航前修复。

如果是一艘悬挂美国旗的船只呢？

类似的规则也适用：如果遵循 2018 年 4 月 16 日 CVC-WI-004(1) 指南解释的 ISM 规则（国际安全管理规则），那船舶将按照《美国联邦法规》颁布的第 33 CFR Part 96 条规章操作。比如，运载超过 12 名乘客; 排水量吨位超过 500GT; 或参加替代性合规项目。还须遵守 CVC-WI-003 指南，其中详细说明了美国海岸警卫队对悬挂美国旗的船舶的安全管理系统的监督。

评论

美国海岸警卫队已明确通知提醒悬挂外国旗船舶的运营者，如果他们在抵达美国港口时没有遵循(哪怕非常基本的)网络安全/网络环境的规定，将面临被扣船的风险，或者至少被要求进行快速补救缺陷。

文件中有迹象表明，网络安全将开始被视为船舶适航的基本条件。同样明确的是，美国海岸警卫队并不关心船舶所悬挂的旗帜，重点是，要么船舶合规，要么是有缺陷需要修理，否则船将被扣留。尚不清楚的是，美国海岸警卫队在他们的指导中为保护环境故意淡化对网络解决方案的要求。

有帮助的是，美国海岸警卫队意识到其他网络风险评估框架的使用(例如 BIMCO 和 ISO/IEC 等其他国际组织所做的工作)。虽然他们显然更偏好“美国国家标准技术研究（NIST）标准”，但认识到 IMO 的评估遵循了 NIST 这一框架的大致方向，因此准备与之合作。

美国海岸警卫队的指南只关注船舶、而没有识别出网络受到入侵的途径，因此该指导在这一点上没有那么有帮助。但尽管如此，指导的要求是明确的，违反的后果也是明确的。

总结

这份指南具有真正的效力。船东应确保每艘船舶均备有明确的文件、标准和程序以确保海事检查员/港口国监督机构对其网络安全风险管理的方法充满信心。在关键系统中即使是最小的故障也需要紧急和专业的补救。如果船舶到达美国港口时关键系统出现故障，将被要求修复并接受审核，并能确保在船舶的下一次到港时得到彻底纠正，否则船舶将被扣留。

以上由 Andrew Liu & Co., Ltd 编译，应以英文为准！

信息来源：The West of England P&I Club