行政命令（EO）14028 下的“关键软件”定义

2021 年 6 月 25 日

介绍

2021 年 5 月 12 日发布的关于改善国家网络安全的第 14028 号行政命令（EO）指示国家标准与技术研究所（NIST）发布关键软件一词的定义。

> *（g）在本命令发布之日起 45 天内，商务部长通过 NIST 局长与国防部长通过 NSA 局长协商，国土安全部长通过 CISA 局长、OMB 局长和国家情报局长协商，应公布术语“关键软件”的定义，以纳入到依据本节第（e）小节发布的指南中。该定义应反映功能所需的特权或访问级别、与其他软件的集成和依赖性、对网络和计算资源的直接访问、对信任至关重要的功能、性能以及如果受到损害的潜在危害。*

EO 指示网络安全和基础设施安全局（CISA）使用已发布的关键软件定义，制定一份属于该定义范围的软件类别和产品的清单，从而符合工程运营部的进一步要求。

> *（h）在本节第（g）小节要求的定义发布后 30 天内，国土安全部长通过 CISA 局长与商务部长通过 NIST 局长协商，应确定并向机构提供一份使用中或采购过程中的软件和软件产品类别清单，该清单符合根据本节第（g）小节发布的关键软件定义。*

为了协调定义及其最终应用，NIST 向社区征集意见书，举办虚拟研讨会收集意见，并与 CISA、管理和预算办公室（OMB）、国家情报局长办公室（ODNI）和国家安全局（NSA）协商制定定义、分阶段实施的概念，以及属于初始阶段范围内的常用软件类别的初步清单。CISA 和 OMB 将为实施 EO 提供更多关于应用该定义的指导。NIST 与 CISA、OMB 密切合作，确保定义和建议与他们的计划一致。

本文从“关键”术语的背景和来源入手，介绍了分阶段方法的概念。它在 EO 的范畴内定义了“关键软件”这一术语，提供了一份符合 EO 定义的初步软件清单，并建议将这些软件列入初步实施阶段。本文最后给出了常见问题解答（FAQ）。CISA 将为初始和未来的实施阶段提供最终的软件范畴。

背景

最近的事件表明，联邦政府需要改进其识别、阻止、防范、检测和响应恶意网络行为和行为者的工作。特别是，威胁行为者正在利用软件使用的普及性、底层代码的复杂性、软件开发和分发实践等。EO 的目标之一是为全联邦政府使用的关键软件产品制定安全基线。将软件指定为“EO 关键”将推动相关活动，包括联邦政府如何购买和管理已部署的关键软件。EO 特别规定，购买软件必须符合 EO 第 4（e）节所界定的安全开发流程和完整性检查等安全措施。

鉴于 EO 的范围广泛及其对政府运作和软件市场的潜在影响，NIST 为关键软件的定义设定了以下目标：

- **明确性：**该计划的实施将推动全联邦政府的活动，并对软件行业产生影响。有一个可供软件行业和政府使用的明确定义，是成功实施 EO 的关键。
- **可行性：**为了使 EO 可行，其实施必须考虑软件行业如何运作，包括产品开发、采购和部署。软件市场是动态且不断发展的。组织对软件的开发、买入和使用方式都在迅速变化。软件是以产品、产品的一部分和服务的形式购买的，通常是由许多组件组成的模块。

“关键”这个术语有许多现有的定义和用法。大多数是基于技术如何支持各种任务或流程，如：“安全关键”或“关键基础设施”。这个术语在 EO 中的使用略有不同，因为它不是基于使用的语境，而是基于一个软件在大多数用例中很可能是关键的这一特性。也就是说，它侧重于处理网络运营和安全基础设施的关键功能。这与高价值资产计划下的联邦民用企业基本信息技术的概念类似。

为了将“关键”一词的常用用法与 EO 下的定义区分开来，在尚未清楚讨论哪种用法时，我们将使用“EO 关键”一词。

方法

考虑到软件市场的规模、范围和复杂性以及政府实施 EO 所需的基础设施，NIST 已就确保“EO 关键软件”供应链的分阶段方法概念与关键机构进行了磋商。这将允许联邦政府和软件行业以渐进的方式实施 EO，从而为每个额外阶段提供反馈和改进流程的机会。

定义与说明材料

本节提供了“EO 关键软件”的定义。下面是一个表格，其中列出了建议初始阶段软件类别的初步清单以及一些解释性材料。稍后，CISA 将提供在定义范围内（包括最初实施阶段）的软件类别的权威列表。如果可用，将在此处提供该信息的指南。

最后，本文底部有一组常见问题解答，回答了可能出现的有关定义解释、分阶段方法和其他相关主题的问题。

“EO 关键软件”被定义为任何具有或直接依赖一个或多个组件的软件，这些组件至少有以下属性之一：

- 被设计运行于高权限或管理权限；
- 能直接或授权访问网络或计算资源；
- 被设计用于控制数据访问或操作技术（OT）；
- 执行“信任的关键”功能；或
- 使用访问权限，在正常信任边界之外执行操作。

该定义适用于，为生产系统购买或部署的，以及用于运营目的的所有形式的软件（例如，独立软件、特定设备或硬件组件的集成软件、基于云的软件）。其他使用情况，如仅用于研究或测试而不部署在生产系统中的软件，不在此定义的范围内。(请参见 FAQ #10 和 FAQ #11）

NIST 建议初始 EO 实施阶段将重点放在具有安全关键功能或有类似重大潜在危害的独立本地软件上。后续阶段可处理其他类别的软件，例如：

- 控制数据访问的软件；
- 基于云的及混合的软件；
- 软件开发工具，如：代码库系统、开发工具、测试软件、集成软件、打包软件和部署软件；
- 引导级固件中的软件组件；或
- 操作技术（OT）中的软件组件。

下表提供了被认为是“EO 关键软件”类别的初步列表。本表是为了说明“EO 关键软件”中定义的应用，以及上述建议的初始实现阶段的范围。如前所述，CISA 稍后将提供软件类别的权威列表。

软件类别	说明	产品类型	纳入的理由
身份、凭证和访问管理（ICAM）	集中识别、验证、管理组织用户、系统和设备的访问权限或执行访问决策的软件	● 身份管理系统 ● 身份提供商和联盟服务 ● 证书颁发者 ● 访问代理 ● 特权访问管理软件 ● 公钥基础设施	● 确保只有授权用户、系统和设备才能访问基础的敏感信息和功能
操作系统、虚拟化程序、容器环境	建立或管理对硬件资源（裸机或虚拟化/容器化）的访问和控制，并向软件应用程序和/或交互用户提供访问控制、内存管理和运行时执行环境等公共服务的软件	● 服务器、桌面和移动设备的操作系统 ● 支持操作系统及类似环境的虚拟程序和容器运营系统	● 具有直接访问和控制底层硬件资源的高度特权软件，并提供最基本和关键的信任和安全功能
Web 浏览器	通过网络处理 web 服务器交付的内容软件，通常用作设备和服务配置功能的用户界面	● 独立和嵌入式浏览器	● 提供多种访问管理功能 ● 支持浏览器插件和扩展，如密码管理器存储凭证的 web 服务器资源 ● 为从远程源代码下载的代码提供执行环境 ● 为存储的内容提供访问管理，例如根据请求提供 web 服务器的访问令牌
终端安全	安装在终端上的软件，通常具有较高的权限，这些权限支持或有助于终端的安全操作，或可手机有关终端的详细信息	● 全磁盘加密 ● 密码管理器 ● 搜索、删除或隔离恶意软件的软件 ● 报告终端安全状态的软件（漏洞和配置） ● 收集有关固件状态、操作系统、应用程序、用户和服务帐户以及运行时环境的详细信息的软件	● 拥有对数据、安全信息和服务的访问特权限，以实现对用户和系统数据的深度检查 ● 提供信任的关键功能

软件类别	说明	产品类型	纳入的理由
网络控制	实现协议、算法以及配置、控制、监视和保护网络中数据流功能的软件	● 路由协议 ● DNS 解析程序和服务器 ● 软件定义的网络控制协议 ● 虚拟专用网（VPN）软件 ● 主机配置协议	● 对关键网络控制功能的特权访问 ● 作为窃取数据的更复杂的第一步，经常被恶意软件破坏
网络保护	防止恶意网络流量进入或离开网段或系统边界的产品	● 防火墙、入侵检测/防范系统 ● 基于网络的策略实施点 ● 应用防火墙和检查系统	● 提供对信任至关重要的功能（通常具有较高的权限）
网络监控和配置	基于网络的监控和管理，能够改变各种系统的状态或安装有代理或特权的软件	● 网络管理系统 ● 网络配置管理工具 ● 网络流量监控系统	● 能够使用提升的权限和/或远程安装的代理监控和/或配置企业 IT 的系统
运行监控和分析	用于报告远程系统的运行状态和安全信息的软件，以及用于处理、分析和响应这些信息的软件	● 安全信息和事件管理（SIEM）系统	● 在远程系统上广泛部署的具有更高权限的软件代理 ● 分析系统对事件检测和响应以及安全事件的根本原因分析至关重要 ● 经常被试图禁用或逃避它的恶意软件攻击
远程扫描	通过对公开的服务执行网络扫描来确定网络终端状态的软件	● 漏洞检测和管理软件	● 通常具有访问网络服务的特权，并收集有关其他系统漏洞的敏感信息
远程访问和配置管理	用于远程系统管理和配置端点或远程控制其他系统的软件	● 策略管理 ● 更新/补丁管理 ● 应用程序配置管理系统 ● 远程访问/共享软件 ● 资产发现和清单系统 ● 移动设备管理系统	● 操作具有重要的访问权限和提升的权限，通常对终端用户的可见性或控制性很低
备份/恢复和远程存储	用于创建副本和传输存储在端点或其他网络设备上的数据的软件	● 备份服务系统 ● 恢复管理器 ● 网络存储（NAS）和存储局域网（SAN）软件	● 对用户和系统数据的特权访问 ● 对网络事件（如勒索软件）后执行响应和恢复功能至关重要

常见问题

以下 FAQ 是与 OMB 和 CISA 协商后编制的，提供了更多的背景资料。

1. **下一阶段什么时候开始？**

   CISA 和 OMB 将在初始阶段监控程序的实施情况，并决定何时纳入其他软件类别。

2. **定义中“直接软件依赖性”是什么意思？**

   对于给定的组件或产品，即直接集成到所讨论的软件实例中并对其进行操作所必需的其他软件组件（如库、包、模块）。这不是依赖关系的系统定义，也不包括其他独立产品的接口和服务。

3. **你在定义中所说的“信任的关键”是什么意思？**

   “信任的关键”包括用于安全功能的软件类别，如网络控制、端点安全和网络保护等。

4. **软件产品是在云环境中、本地环境中还是在混合环境中，这有关系吗？**

   不。如果一个产品或服务提供的功能属于“EO 关键”定义的一部分，那么无论其部署模式如何，该产品或服务本身都是“EO 关键”的。尽管如此，NIST 建议在 EO 的初始阶段，将重点放在本地软件上。许多本地产品依赖于基于云的组件和服务来执行“EO 关键”功能（例如，基于云的访问控制）。在这种情况下，如果本地组件直接执行“EO 关键”功能，则它们在范围内。建议在实施的后期阶段处理基于云的组件和系统，以便有时间与此类系统的其他联邦要求（如 FedRAMP）进行协调。

5. **开源软件能成为“E0 关键”吗？**

   能。如果开源软件执行的功能被定义为“EO 关键”，那么它就是“EO 关键”。在实践中，开源软件经常被合并到其他产品中。在这种情况下，产品开发人员将把开源组件视为自己开发过程的一部分。而在其他情况下，开源软件是一个独立的产品。在这种情况下，仍然适用 EO 的要求。如果支持该产品的开源社区没有或不能满足第 4（e）节中的某些要求，政府则可能需要自行解决。

6. **政府开发的软件能成为“E0 关键”吗？**

   联邦政府通过内部和合同开发软件。而这些产品通常被称为 GOTS（政府现成的）软件。如果 GOTS 软件执行的功能包含在“EO 关键”定义中，那么他就是“EO 关键”的。虽然 EO 第 4 节未对商业软件和 GOTS 软件进行区分，但根据 GOTS 软件的开发和采购方式，可能会与需要在 EO 条件下为关键软件开发的标准和程序有所不同。

7. 如果一个产品部分是“EO 关键”，而部分不是呢？

如果一个产品的构成功能是包含在“EO 关键”定义中的，那么产品本身就是“EO 关键”。然而，某些“EO 关键软件”产品可以包含不同的组件，这些组件不具备“EO 关键”属性或不直接支持产品提“EO 关键”功能。当开发人实证明第 4（e）节中的安全措施时，他们可以指定其产品的哪些组件是“EO 关键”的、哪些是不符合的，并满足符合第 4（e）节中的安全要求。虽然这可能会导致供应商对如何确定其认证范围有不同的解释，但其目的是要求供应商明确哪些组件得到认而证，哪些组件没有得到认证。

8. 如果软件是作为另一个产品的组件购买的呢？

如果产品执行的功能属于“EO 关键”定义的一部分，那么产品本身就是“EO 关键”的。当供应实证明实施了第 4（e）节规定的安全措施时，他们指定说明其产品的组件被覆盖保护。这些可能包括由其他各方开发的组件。例如，如果政府购买了一个包含操作系统的产品，且该产品是“EO 关键”的，则需要对安全措施进行认证，但认证仅限于操作系统。详见 FAQ #7。

9. 这将如何与 FedRAMP 协同？

EO 第 3 节论述了 FedRAMP 的现代化。建议的分阶段方法是从内部部署软件开始，并理解一些基于云托管组件的内部部署软件可能也在范围之内。CISA 将与 FedRAMP 协调，在实施的后期阶段确定 EO 对基于云的软件的范围和适用性。

10. 该定义不包括出于操作目的而不会部署在生产系统中的软件。能提供更多的解释吗？

有几个用例，在这些用例中，软件是有的，但部署的方式不足以构成重大的危害风险。例如，包括用作研究目的的软件和为存档目的收集的软件。这将允许政府出于非操作用途，购买那些供应商没有实施或证明 4(e)中的安全措施的“EO 关键软件”。

11. 国家安全系统（NSS）中使用的软件如何？覆盖它们吗？

EO 第 9 节描述了 EO 要求对国家安全系统的适用性。

12. 嵌入式软件或固件可以是“EO 关键”的吗？

是的。如果嵌入式软件或固件的功能被定义为“EO 关键”的，那么它就是“EO 关键”的。由于此类产品的复杂性，我们建议在实施的初始阶段不要包含此类软件。

13. 难道部门和机构不应该根据软件对支持机构使命的方式来决定什么是“EO 关键”的吗?

不。“EO 关键”的定义是基于软件的功能，而不是它的用途。这将有利于软件供应商判断他们的产品是否是“EO 关键”的，而和个别的采购或部署情况无关，因此他们可以满足第 4(e)节的要求。这也将使市场更加清晰。否则，政府可能

会寻求购买某个产品，但没有供应商预期该产品是“EO 关键”的，从而导致政府没有或仅有有限的产品可供购买。表中定义的软件类型在大多数情况下可能是“EO 关键”的。

14. 那么“安全关键”和其他“高保证”系统该如何呢？

有许多类型的“安全关键”和其他“高保证”系统。它们中，有许多都被监管或有相关行业安全需求。如果这些系统使用的软件包含“EO 关键”功能，那么该软件就是“EO 关键”的。“安全关键”和 “高保证”的软件和系统会有补充的安全要求。例如，如果一个“高保证”系统包含一个操作系统，该操作系统是“EO 关键”的，除了满足“安全关键”或其他系统要求外，还必须满足“EO 关键”要求。

15. 如果我使用的软件产品没有包含在“E0 关键”清单中，但它对我是很关键的，我可以要求供应商提供证明吗？

是的，各部门和机构可以利用第 4（e）节中定义的“EO 关键”安全措施作为采购的一部分。