天融信
TOPSEC
证券代码:002212

相融共创 赋能未来

融信译站

根据行政命令（EO）14028

“EO 关键软件”应用的安全措施

天融信科技集团

介绍

2021 年 5 月 12 日关于改善国家网络安全的第 14028 号行政命令(EO)指示，美国国家标准与技术研究所(NIST)根据 NIST 为 EO 开发的“EO 关键软件”的定义，发布了关于“EO 关键软件”应用的安全措施指南。

> *(i)在本命令发出之日起 60 天内，商务部代理部长（通过 NIST 局长）与国土安全部部长（通过 CISA 局长和 OMB 局长）协商，应发布概述本节第(g)款中定义的“关键软件”的安全措施的指南，包括应用最小特权、网络分段以及适当配置。*

EO 指示管理和预算办公室(OMB)要求各机构遵守安全措施指南。

> *(j)在本节第(i)款所述指南发布后的 30 天内，OMB 局长应通过 OMB 电子政府办公室行政长官采取适当步骤，要求各机构遵守该指南。*

为了帮助确定可纳入的安全措施及其优先次序，NIST 向社区征集了立场文件、主办了一个收集意见的虚拟研讨会、咨询了网络安全和基础设施安全局(CISA)和 OMB、在现有联邦指导意见中审查了可能适用于“EO 关键软件”应用的个别安全措施。

本文件首先介绍了指南的目的和范围，包括“EO 关键软件应用”的含义。其次，定义了“EO 关键软件”应用的基本安全措施。它以常见问题(FAQ)结尾，提供了关于指南及其与 EO 其他任务、其他联邦网络安全计划之间关系的更多信息。FAQ 中的最后一项是安全措施的总结。

指导目的和范围

最近的事件表明，有必要更好地保护联邦机构在本地、云和其他地方使用的“EO 关键软件”，以实现其任务。即使“EO 关键软件”开发时可以应用推荐的安全开发实践，但它仍需要在操作环境中得到保护。越来越多的人认识到，所有组织都应该假设违规行为将要发生或已经发生，所以必须在任何时候都把“EO 关键软件”的访问限制在所需范围内。此外，必须持续监控异常或恶意活动。防止违规仍然是“必须”的，但拥有强大的事件检测、响应和恢复能力也同样重要。这种能力有助于识别漏洞、确定其影响范围、发现根本原因、并迅速恢复正常运作，从而最大限度地减少对机构任务的干扰。
本安全措施指南适用于联邦机构对“EO 关键软件”的使用场景。“EO 关键软件”的开发和采购不在范围内。这些安全措施旨在保护各机构运行环境中已部署的“EO 关键软件”的使用过程。NIST 为安全措施定义了以下目标:

1. 保护“EO 关键软件”和“EO 关键软件平台”（运行“EO 关键软件”的平台，如终端、服务器、云资源等）免受未经授权的访问和使用。
2. 保护“EO 关键软件”和“EO 关键软件平台”使用的数据的机密性、完整性和可用性。（参见 FAQ#6）
3. 识别和维护“EO 关键软件平台”和部署在这些平台上的软件，以保护“EO 关键软件”免被利用。
4. 快速检测、响应和恢复涉及“EO 关键软件”和“EO 关键软件平台”的威胁和事件。
5. 加强对人员行为的理解和绩效，促进“EO 关键软件”和“EO 关键软件平台”的安全性。

NIST 已经确定了满足这些目标的基本安全措施。这些“EO 关键软件应用的安全措施”并无意做到全面，也无意消除其他安全措施（联邦机构现有要求和网络安全计划）的必要性。各机构应继续努力确保运行“EO 关键软件”的系统和网络的安全，并管理网络供应链风险（参见 FAQ#4），以及实施零信任实践（参见 FAQ#5），这取决于基本的安全措施。指定这些安全措施的目的是，通过定义一组通用的安全目标，来帮助机构确定其安全措施落实的优先级，进而保护“EO 关键软件”的使用过程。

“E0关键软件”应用的安全措施

下表定义了“EO 关键软件”应用的安全措施并按目标分组。表中的列为：

- **安全措施(SM)：**一种高级安全结果声明，旨在适用于所有被指定为“EO 关键软件”的软件或运行它的所有平台、用户、管理员、数据或网络（如指定）。
- **联邦政府参考资料：**联邦政府发布的全部或部分讨论安全措施的出版物和项目。每种安全措施的前两个参考文献是 NIST 网络安全框架和 NIST 特别出版物(SP)800-53 第 5 版-信息系统和组织的安全与隐私控制。这两个引用列出了它们到安全措施的映射（分别作为网络安全框架子类别和 SP 800-53 安全控制）。这些映射具有通用性和信息性，任何特定情况都可能有不同的映射。

前两项后的所有引用都是讨论或说明安全措施的选定示例，并同时作为可能的信息来源。而有些引用仅适用于特定的用例、环境、情况等。在此列表中省略并不意味着不应使用其他信息来源。

表中所列的参考文献将随着新出版物的确定或发行以及现有出版物的更新而定期更新。

表中使用的缩略语为：

- **CISA：** 网络安全与基础设施安全局
- **DISA：** 国防信息系统局
- **GSA：** 总务管理局
- **NIST：** 国家标准与技术研究院
- **NSA：** 国家安全局
- **OMB：** 管理与预算办公室

安全措施(SM)	联邦政府参考资料
目标 1：保护“EO 关键软件”和“EO 关键软件平台”免受未经授权的访问和使用。	
SM 1.1:对“EO 关键软件”和“EO 关键软件平台”的**所有用户和管理员采用多因素身份验证，该身份验证应能抗伪造。**（参见 FAQ#7）	▪ **NIST**，网络安全框架：PR.AC-1，PR.AC-7 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AC-2、IA-2、IA-4、IA-5 ▪ **CISA**，不良行为 ▪ **CISA**，能力增强指南：实现强身份验证 ▪ **CISA**，CDM 项目仪表盘生态系统 ▪ **CISA**，持续诊断和缓和计划：身份和访问管理-谁在网络上？ ▪ **GSA**，联邦身份、凭证和访问管理(FICAM)体系结构 ▪ **GSA**，IDManagement.gov ▪ **NIST**，特权用户 PIV 认证的最佳实践 ▪ **NIST**，SP 800-63-3，数字身份指南 ▪ **NIST**，SP 800-157，衍生个人身份验证(PIV)凭证指南 ▪ **NIST**，SP 1800-12，衍生个人身份验证(PIV)凭证 ▪ **NIST**，SP 1800-17，电子商务的多因素认证：基于风险，采购方 FIDO 通用第二因素实践 ▪ **NSA**，选择安全的多因素认证解决方案 ▪ **NSA**，过渡到多因素认证 ▪ **OMB**，备忘录 M-19-17，通过改进身份、证书和访问管理实现任务交付
SM 1.2：唯一标识并鉴别试图访问“EO 关键软件”或“EO 关键软件平台”的**每个服务**。	▪ **NIST**，网络安全框架：PR.AC-1、PR.AC-7 ▪ **NIST**， SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AC-2，IA-9 ▪ **CISA**，不良行为
SM 1.3：对基于网络的“EO 关键软件”或“EO 关键软件平台”**管理，应遵循特权访问管理原则**。可能的实现示例包括：每次使用前应采用专门用于管理和验证的加固平台；要求每个管理员具有唯一标识；以及代理并记录“EO 关键软件平台”的所有管理会话。	▪ **NIST**，网络安全框架：PR.AC-1、PR.AC-7、PR.MA-1、PR.MA-2 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AC-2、IA-2、SC-2、SC-7 增强 15 ▪ **CISA**，保护高价值资产 ▪ **CISA**，保护网络基础设施设备
SM 1.4：采用适当的边界保护技术，尽量减少对“EO 关键软件”、“EO 关键软件平台”和相关数据的直接访问。这类技术的例子包括：网络分段、隔离、软件定义的边界和代理。	▪ **NIST**，网络安全框架：PR.AC-3、PR.AC-5 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：SC-7 ▪ **CISA**，持续诊断和缓解计划：网络安全管理-网络上发生了什么？如何保护网络？

安全措施(SM)	联邦政府参考资料
	▪ **CISA**，防范软件供应链攻击 ▪ **CISA**，保护网络基础设施设备 ▪ **CISA**，可信互联网连接 3.0：传统 TIC 用例 ▪ **NIST**，SP 800-41 第 1 版，防火墙和防火墙政策指南 ▪ **NIST**，SP 800-207，零信任体系架构 ▪ **NSA**，分段网络和部署应用程序感知防御
目标 2：保护“EO 关键软件”和“EO 关键软件平台”使用的数据的机密性、完整性和可用性。（参见 FAQ#6）	
SM 2.1：建立并维护“EO 关键软件”和“EO 关键软件平台”的**数据清单**。	▪ **NIST**，网络安全框架：ID.AM-3，DE.AE-1 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：CM-8、PM-5 ▪ **CISA**，持续诊断和缓解计划：数据保护管理-如何保护数据？ ▪ **CISA**，防范软件供应链攻击 ▪ **CISA**，软件资产管理的 FAQ ▪ **GSA**，清单.数据.域名指南 ▪ **NIST**，数据分级分类项目 ▪ **OMB**，备忘录 M-16-12，类别管理政策 16-1：改善通用信息技术的获取和管理：软件许可
SM2.2：对“EO 关键软件”和“EO 关键软件平台”所使用的数据和资源**进行细粒度访问控制**，尽可能执行最小特权原则。	▪ **NIST**，网络安全框架：PR.AC-4 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AC-2、AC-3、AC-6 ▪ **CISA**，持续诊断和缓解计划：身份和访问管理-谁在网络上？ ▪ **CISA**，QSMO 服务–身份管理和访问控制 ▪ **NIST**，SP 800-162，基于属性访问控制(ABAC)定义和注意事项指南 ▪ **NIST**，SP 800-205，访问控制系统的属性考虑 ▪ **NIST**，SP 800-207，零信任体系架构
SM 2.3：保护静态数据，对“EO 关键软件”和“EO 关键软件平台”使用的敏感数据，采用符合 NIST 标准的加密。	▪ **NIST**，网络安全框架：PR.DS-1 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：SC-28 ▪ **CISA**，持续诊断和缓解计划：数据保护管理-如何保护数据？ ▪ **CISA**，基于多层数据保护策略的网络数据保护 ▪ **NIST**，SP 800-111，终端用户设备存储加密技术指南 ▪ **NIST**，SP 800-175B 第 1 版，联邦政府密码标准使用指南：密码机制 ▪ **NIST**，SP 800-209，存储基础结构安全指南 ▪ **OMB**，通告 A-130，附录 I,4.i.14

安全措施(SM)	联邦政府参考资料
SM 2.4：保护传输中的数据，对“EO 关键软件”和“EO 关键软件平台”的敏感数据通信，在可行的情况下采用双向鉴别，以及符合 NIST 标准的加密。	▪ **NIST**，网络安全框架：PR.AC-3、PR.AC-7、PR.DS-2、PR.PT-4、DE.CM-7 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AC-4、AC-17、SC-8 ▪ **CISA**，持续诊断和缓解计划：数据保护管理-如何保护数据？ ▪ **CISA**，基于多层数据保护策略的网络数据保护 ▪ **NIST**，SP 800-46 第 2 版，企业远程办公、远程访问和自带设备(BYOD)安全指南 ▪ **NIST**，SP 800-47 第 1 版，管理信息交流安全 ▪ **NIST**，SP 800-52 第 2 版，传输层安全(TLS)实现的选择、配置和使用指南 ▪ **NIST**，SP 800-77 第 1 版，IPsec VPN 指南 ▪ **NIST**，SP 800-175B 第 1 版，联邦政府密码标准使用指南：密码机制 ▪ **NSA**，消除过时的传输层安全(TLS)协议配置 ▪ **OMB**，通告 A-130，附录 I,4.i.14 ▪ **OMB**，备忘录 M-15-13，要求跨联邦网站和网络服务安全连接的政策
SM 2.5：备份数据，执行恢复演练，随时**准备**从备份中**恢复**“EO 关键软件”和“EO 关键软件平台”使用的**数据**。	▪ **NIST**，网络安全框架：PR.IP-4 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：CP-9、CP-10 ▪ **NIST**，SP 800-34 第 1 版，联邦信息系统应急计划指南 ▪ **NIST**，SP 800-57 第 5 版，密钥管理建议：第 1 部分：概述 ▪ **NIST**，SP 800-175B 第 1 版，联邦政府密码标准使用指南：密码机制
目标 3：识别和维护“EO 关键软件平台”和部署在这些平台上的软件，以保护“EO 关键软件”免被利用。	
SM 3.1：建立和维护软件清单，包括所有运行的“EO 关键软件平台”和部署到这些平台的所有软件（EO 关键和非 EO 关键）。	▪ **NIST**，网络安全框架：ID.AM-1、ID.AM-2、ID.SC-2 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：CM-8、PM-5、RA-9 ▪ **CISA**，CDM 项目仪表盘生态系统 ▪ **CISA**，CDM 软件资产管理(SWAM)能力 ▪ **CISA**，持续诊断和缓解计划：资产管理-网络上有什么？ ▪ **CISA**，防范软件供应链攻击 ▪ **NIST**，IR 8011 第 3 卷，自动化支持安全控制评估：软件资产管理 ▪ **NIST**， SP 1800-5，IT 资产管理

安全措施(SM)	联邦政府参考资料
SM 3.2：采取补丁管理实践维护“EO 关键软件平台”和部署到这些平台的所有软件。 实践包括： ▪ 快速识别、记录和缓解已知漏洞（例如：打补丁、更新、将软件升级到支持的版本），以持续减少暴露时间 ▪ 监控平台和软件，以确保不会将缓解措施遗漏在变更控制流程之外	▪ **NIST**，网络安全框架：ID.RA-1、ID.RA-2、ID.RA-6、PR.IP-12、DE.CM-8、RS.MI-3 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：CA-7、RA-5、SI-2、SI-5、SR-8 ▪ **CISA**，不良行为 ▪ **CISA**，能力增强指南：远程漏洞和补丁管理 ▪ **CISA**，CDM 项目仪表盘生态系统 ▪ **CISA**，持续诊断和缓解计划：资产管理-网络上有什么？ ▪ **CISA**，防范软件供应链攻击 ▪ **NIST**，IR 8011 第 4 卷，自动化支持安全控制评估：软件漏洞管理 ▪ **NIST**，修补企业项目 ▪ **NIST**，SP 800-40 第 3 版，企业补丁管理技术指南
SM 3.3：采取配置管理实践来维护“EO 关键软件平台”和部署到这些平台的所有软件。 实践包括： ▪ 为每个“EO 关键软件平台”和部署到该平台的所有软件确定适当的强化安全配置（强化安全配置执行最小特权、职责分离和功能最少的原则） ▪ 实施平台和软件的配置 ▪ 控制和监控平台和软件，确保配置不会在变更控制过程之外发生变更	▪ **NIST**，网络安全框架：ID.RA-1、ID.RA-2、ID.RA-6、PR.AC-4、PR.IP-1、PR.IP-3、PR.PT-3、DE.CM-8、RS.MI-3 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AC-5、AC-6、CA-7、CM-2、CM-3、CM-6、CM-7、RA-5、SI-5 ▪ **CISA**，CDM 项目仪表盘生态系统 ▪ **CISA**，持续诊断和缓解计划：资产管理-网络上有什么？ ▪ **CISA**，防范软件供应链攻击 ▪ **DISA**，STIGs 文档库 ▪ **NIST**，国家检查表计划(NCP)检查表库 ▪ **NIST**，SP 800-70 第 4 版，国家 IT 产品清单计划：清单用户和开发人员指南 ▪ **NIST**，SP 800-128，信息系统安全配置管理指南
目标 4：快速检测、响应和恢复涉及“EO 关键软件”和“EO 关键软件平台”的威胁和事件。	
SM 4.1：配置日志记录，记录涉及“EO 关键软件平台”和在这些平台上运行的所有软件的**安全事件的必要信息**。	▪ **NIST**，网络安全框架：PR.PT-1 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AU-2、AU-3、AU-4、AU5、AU-8、AU-9、AU-11、AU-12 ▪ **CISA**，持续诊断和缓解计划：网络安全管理-网络上发生了什么？如何保护网络？ ▪ **CISA**，发现和纠正恶意活动的技术方法 ▪ **NIST**，国家检查表计划(NCP)检查表库 ▪ **NIST**，SP 800-92，计算机安全日志管理指南 ▪ **OMB**，通告 A-130，附录 I,4.i.7

安全措施(SM)	联邦政府参考资料
SM 4.2：持续监控“EO 关键软件平台”和所有在这些平台上运行的软件的**安全性**。	▪ **NIST**，网络安全框架：DE.CM-7 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：CA-7，SI-4 ▪ **CISA**，持续诊断和缓解(CDM) ▪ **CISA**，防范软件供应链攻击 ▪ **NIST**，IR 8011 第 3 卷，自动化支持安全控制评估：软件资产管理 ▪ **NIST**，SP 800-137，联邦信息系统和组织的信息安全持续监控(ISCM)
SM 4.3：在“EO 关键软件平台”上**采用终端安全保护**，保护平台及其上运行的所有软件。 功能包括： ▪ 通过识别、评估、最小化攻击面和已知的威胁暴露，来保护软件、数据和平台 ▪ 只允许执行经过验证的软件（例如：文件完整性校验、可执行文件签名、白名单） ▪ 主动检测威胁，并在可能的情况下阻止它们 ▪ 响应事件并从事件中恢复 ▪ 为安全运营、威胁狩猎、事件响应和其他安全需求提供必要的信息	▪ **NIST**，网络安全框架：PR.DS-5、PR.DS-6、DE.AE-2、DE.CM-4、DE.CM-7、DE.DP-4 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：SI-3、SI-4、SI-7 ▪ **CISA**，持续诊断和缓解计划：数据保护管理-如何保护数据？ ▪ **CISA**，防范软件供应链攻击 ▪ **NIST**，SP 800-61 第 2 版，计算机安全事故处理指南 ▪ **NIST**，SP 800-83 第 1 版，桌面和笔记本电脑恶意软件事件预防和处理指南 ▪ **NIST**，SP 800-150，网络威胁信息共享指南 ▪ **NIST**，SP 800-167，应用程序白名单指南 ▪ **NIST**，SP 800-184，网络安全事件恢复指南 ▪ **NSA**，强制执行已签名的软件执行策略
SM 4.4：采用网络安全保护，监控进出“EO 关键软件平台”的网络流量，保护使用网络的平台及其软件。 功能包括： ▪ 主动检测所有堆栈层的威胁，包括应用程序层，并在可能的情况下阻止它们 ▪ 为安全运营、威胁狩猎、事件响应和其他安全需求提供必要的信息	▪ **NIST**，网络安全框架：PR.DS-5、DE.AE-1、DE.AE-3、DE.CM-1、DE.CM-4、DE.CM-7、DE.DP-4 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AU-13、AU-14、SC-7、SI3 ▪ **CISA**，持续诊断和缓解计划：数据保护管理-如何保护数据？ ▪ **CISA**，持续诊断和缓解计划：网络安全管理-网络上发生了什么？如何保护网络？ ▪ **CISA**，防范软件供应链攻击 ▪ **CISA**，保护网络基础设施设备 ▪ **CISA**，可信互联网连接 3.0:传统 TIC 用例 ▪ **NIST**，SP 800-41 第 1 版，防火墙和防火墙政策指南 ▪ **NIST**，SP 800-61 第 2 版，计算机安全事件处理指南 ▪ **NIST**，SP 800-94 第 1 版，入侵检测和预防系统(IDPS)指南

安全措施(SM)	联邦政府参考资料
SM 4.5：针对所有安全运营人员和事件响应团队成员，根据其角色和职责，培训如何处理涉及“EO 关键软件”和“EO 关键软件平台”的事件。	▪ **NIST**，网络安全框架：PR.AT-5、PR.IP-9、PR.IP-10 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AT-3、CP-3、IR-2 ▪ **CISA**，事故响应培训 ▪ **NIST**，SP 800-61 第 2 版，计算机安全事件处理指南 ▪ **NIST**，SP 800-181 第 1 版，网络安全劳动力框架（NICE 框架）
目标 5：加强对人员行为的理解和绩效，促进“EO 关键软件”和“EO 关键软件平台”的安全性。	
SM 5.1：针对“EO 关键软件”的所有用户，根据其角色和职责，培训如何安全地使用软件和“EO 关键软件平台”。	▪ **NIST**，网络安全框架：PR.AT-1 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AT-2、AT-3 ▪ **CISA**，PCII 授权用户培训 ▪ **NIST**，SP 800-181 第 1 版，网络安全劳动力框架（NICE 框架）
SM 5.2：针对所有“EO 关键软件”和“EO 关键软件平台”的管理员，根据其角色和职责，培训如何安全地管理软件和/或平台。	▪ **NIST**，网络安全框架：PR.AT-2 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AT-3、CP-3 ▪ **NIST**，SP 800-181 第 1 版，网络安全劳动力框架（NICE 框架）
SM 5.3：经常开展宣传活动，加强对“EO 关键软件和平台”的所有用户和管理员的培训，并衡量培训的有效性，以便持续改进。	▪ **NIST**，网络安全框架：PR.AT-1、PR.AT-2 ▪ **NIST**，SP 800-53 第 5 版，信息系统和组织的安全与隐私控制：AT-3 ▪ **CISA**，网络教育与意识 ▪ **NIST**，SP 800-181 第 1 版，网络安全劳动力框架（NICE 框架）

常见问题FAQs

以下常见问题解答提供了有关指南的附加信息。

1. **所有安全措施是否适用于所有“EO 关键软件”？**

基于软件部署的性质或其他因素，安全措施可能与特定情况无关。如果无法实施某一特定的安全措施，则可以识别并实施其他安全措施来降低风险，以达到缺失的安全措施所应达到的效果。各机构仍需将风险管理活动作为其整体网络安全计划的一部分。

2. **本指南是否会因更多类型的“EO 关键软件”被识别出来而更新？**

可能会，然而，“EO 关键软件”的安全措施预计将适用于所有部署中的所有类型的“EO 关键软件”。

3. 我们如何实施基于云的“EO 关键软件”的安全措施？

为了支撑 EO 第 3 节，CISA、GSA 的 FedRAMP 计划和 OMB 目前正在开发联邦云安全战略和云安全技术参考体系架构文档。云服务提供商可以将“EO 关键软件”的安全措施应用到基于云的环境中。

4. NIST 在网络供应链风险管理(C-SCRM)方面是否有额外的资源？

是的，请参阅 NIST 的 C-SCRM 项目网站，获得所有资源的链接。例如，NIST 主办的联邦 C-SCRM 论坛；该论坛促进联邦机构之间的合作和 C-SCRM 信息交流，提高了联邦供应链的安全性。NIST C-SCRM 指南的例子包括 SP 800-161，《联邦信息系统和组织的供应链风险管理实践》和 SP 800-161 修订版 1（草案）以及《系统和组织的网络供应链风险管理实践》。

5. 本指南与零信任架构之间的关系是什么？

EO 的第 3 节指示每个联邦机构计划实施零信任架构。尽管它们不完整，本指南中定义的所有“EO 关键软件”的安全措施也是零信任体系结构的组成部分。制定迁移到零信任体系结构计划的机构可以将“EO 关键软件”应用的安全措施纳入这些计划中。有关零信任体系结构的更多信息，请参阅以下联邦政府资源：

- *DISA 和 NSA，《国防部(DoD)零信任参考体系结构 1.0 版》*
- *NIST，SP 800-207，《零信任体系结构》*
- *NSA，《拥抱零信任安全模型》*

6. 目标 2 说的是“保护数据的机密性、完整性和可用性”，但对于不需要这三者的情况，比如保护公开信息的机密性，又该怎么办？

各机构应继续采取基于风险的方法来保护数据，因此应仅适用于可降低特定场景风险的保护类型。例如，保护公开信息的机密性通常不会降低风险，因此没有必要。

7. SM 1.1 包含术语“抗验证伪造”。这是什么意思？

抗验证伪造的身份认证协议和证书确保当用户或管理员试图通过网络连接到“EO 关键软件”或“EO 关键软件平台”时，双方（个人和平台）都是合法的。抗验证伪造有助于防止网络钓鱼攻击窃取用户的认证信息，也有助于防止攻击者利用窃取的身份验证信息来冒充用户或管理

员。有几种方法可以实现抗验证伪造；抗验证伪造协议的一个例子是客户端认证传输层安全(TLS)。参见 NIST SP 800-63B 第 5.2.5 节了解更多信息。

8. 我在哪里可以了解更多有关“EO 关键软件”的信息？

更多信息请浏览此网页。它包括一组常见问题(FAQs)解答，提供了有关“EO 关键软件”的更多详细信息和相关环境。

9. 是否有安全措施摘要？

有的，下面的清单包括每项安全措施的第一句话。本摘要旨在提高对安全措施的理解，并不能替代上表中对“EO 关键软件”应用的安全措施的正式定义，上表包含了一些安全措施的更多细节，并为所有安全措施提供了有用的参考资料。

目标 1：保护“EO 关键软件”和“EO 关键软件平台”免受未经授权的访问和使用。

- **SM 1.1：**对“EO 关键软件”和“EO 关键软件平台”的**所有用户和管理员采用多因素身份验证，该身份验证应能抗伪造。**（参见 FAQ#7）
- **SM 1.2：唯一标识并鉴别**试图访问“EO 关键软件”或“EO 关键软件平台”的**每个服务**。
- **SM 1.3：对基于网络的**“EO 关键软件”或“EO 关键软件平台”**管理，应遵循特权访问管理原则**。
- **SM 1.4：采用适当的边界保护技术**，尽量减少对“EO 关键软件”、“EO 关键软件平台”和相关数据的直接访问。

目标 2：保护“EO 关键软件”和“EO 关键软件平台”使用的数据的机密性、完整性和可用性。

- **SM 2.1：建立和维护**“EO 关键软件”和“EO 关键软件平台”的**数据清单**。
- **SM2.2：**对“EO 关键软件”和“EO 关键软件平台”所使用的数据和资源**进行细粒度访问控制**，尽可能执行最小特权原则。
- **SM 2.3：保护静态数据，**对“EO 关键软件”和“EO 关键软件平台”使用的敏感数据，采用符合 NIST 标准的加密。

- **SM 2.4：保护传输中的数据，**对“EO 关键软件”和“EO 关键软件平台”的敏感数据通信，在可行的情况下采用双向鉴别，以及符合 NIST 标准的加密。
- **SM 2.5：备份数据，执行恢复演练，**随时**准备**从备份中**恢复**“EO 关键软件”和“EO 关键软件平台”使用的**数据**。

目标 3：识别和维护“EO 关键软件平台”和部署在这些平台上的软件，以保护“EO 关键软件”免被利用。

- **SM 3.1：建立和维护软件清单，**包括所有运行的“EO 关键软件平台”和部署到这些平台的所有软件（EO 关键和非 EO 关键）。
- **SM 3.2：采取补丁管理实践**维护“EO 关键软件平台”和部署到这些平台的所有软件。
- **SM 3.3：采取配置管理实践来维护**“EO 关键软件平台”和部署到这些平台的所有软件。

目标 4：快速检测、响应和恢复涉及“EO 关键软件”和“EO 关键软件平台”的威胁和事件。

- **SM 4.1：配置日志记录，记录涉及**“EO 关键软件平台”和在这些平台上运行的所有软件的**安全事件的必要信息**。
- **SM 4.2：持续监控**“EO 关键软件平台”和所有在这些平台上运行的软件的**安全性**。
- **SM 4.3：**在“EO 关键软件平台”上**采用终端安全保护，**保护平台及其上运行的所有软件。
- **SM 4.4：采用网络安全保护，**监控进出“EO 关键软件平台”的网络流量，保护使用网络的平台及其软件。
- **SM 4.5：针对所有安全运营人员和事件响应团队成员，根据其角色和职责，**培训如何处理涉及“EO 关键软件”和“EO 关键软件平台”的事件。

目标 5：加强对人员行为的理解和绩效，促进“EO 关键软件”和“EO 关键软件平台”的安全性。

- **SM 5.1：针对“EO 关键软件”的所有用户，根据其角色和职责，**培训如何安全地使用软件和“EO 关键软件平台”。
- **SM 5.2：针对所有“EO 关键软件”和“EO 关键软件平台”的管理员，根据其角色和职责，**培训如何安全地管理软件和/或平台。

- **SM 5.3：经常开展宣传活动**，加强对“EO 关键软件和平台”的所有用户和管理员的培训，并衡量培训的有效性，以便持续改进。