Check for updates

NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Check for updates

NIST 特别出版物 800
NIST SP
800-171r3

保护非联邦系统中的受控非机密信息及组织

罗恩·罗斯
维多利亚·皮利特里

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-171r3

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

May 2024



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST 特别出版物 800
NIST SP
800-171r3

保护非联邦系统中的受控非机密信息及组织

罗恩·罗斯
维多利亚·皮利特里
计算机安全部
信息技术实验室

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-171r3

2024年5月



美国商务部
吉娜·M·雷蒙多，部长

美国国家标准与技术研究院
*Laurie E.Locascio,NIST*主任兼商务部标准与技术副部长

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority
This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-04-23
Supersedes NIST Special Publication 800-171r2 (February 2020; Includes updates as of 01-28-2021)
https://doi.org/10.6028/NIST.SP.800-171r2

How to Cite this NIST Technical Series Publication:
Ross R, Pillitteri V (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3

Author ORCID iDs
Ron Ross: 0000-0002-1099-9757
Victoria Pillitteri: 0000-0002-7446-7506

本文中标识了某些设备、仪器、软件或材料(商业或非商业)，以充分说明实验程序。此类标识并不意味着NIST推荐或认可任何产品或服务，也不意味着所标识的材料或设备必然是用于该目的的最佳可用选择。

本出版物中可能引用了NIST根据其法定职责正在制定的其他出版物。本出版物中的信息，包括概念和方法，联邦机构甚至可以在这些配套出版物完成之前使用。因此，在每份出版物完成之前，现有的要求、指南和程序(如存在)仍然有效。出于规划和过渡目的，联邦机构不妨密切关注NIST这些新出版物的制定进展。

鼓励组织在公开评论期内审阅所有草案出版物并向NIST提供反馈。许多NIST网络安全出版物(除上述所列之外)可在https://csrc.nist.gov/publications.获取

权限
本出版物由NIST根据2014年《联邦信息安全管理法》(FISMA)、44 U.S.C.3551 et seq.、公法(P.L.)113-283规定的法定职责制定。NIST负责制定信息安全标准和指南，包括联邦信息系统的最低要求，但此类标准和指南未经对此类系统行使政策权力的适当联邦官员明确批准，不得适用于国家安全系统。本指南与管理和预算办公室(OMB)A-130号通告的要求一致。

本出版物中的任何内容均不得被视为与商务部长根据法定权力强制联邦机构遵守的标准和指南相抵触。这些指南也不应被解释为改变或取代商务部长、OMB主任或任何其他联邦官员的现有权力。本出版物可由非政府组织自愿使用，在美国不受版权保护。但NIST希望在使用时予以注明出处。

NIST 技术系列政策
版权、使用和许可声明
NIST技术系列出版物标识符语法

出版历史
2024-04-23 经 NIST 编辑审查委员会批准
取代NIST特别出版物800-171r2(2020年2月；包含截至01-28-2021的更新)https://doi.org/10.6028/NIST.SP.800-171r2

如何引用本 NIST 技术系列出版物：
Ross R, Pillitteri V(2024)《保护非联邦系统与组织中的受控非机密信息》。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP)NIST SP 800-171r3。https://doi.org/10.6028/NIST.SP.800-171r3

作者 ORCID iD
Ron Ross：0000-0002-1099-9757
维多利亚·皮利特里：0000-0002-7446-7506

Submit Comments
800-171comments@list.nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/171/r3/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

800-171comments@list.nist.gov
美国国家标准与技术研究院
收件人：计算机安全部，信息技术实验室 100 Bureau Drive(Mail Stop 893

附加信息
有关本出版物的更多信息可在https://csrc.nist.gov/pubs/sp/800/171/r3/final，获取，包括相关内容、潜在更新和文

所有评论均须根据《信息自由法》(FOIA) 予以公开。

Abstract

The protection of Controlled Unclassified Information (CUI) is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations. The requirements apply to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This publication can be used in conjunction with its companion publication, NIST Special Publication 800-171A, which provides a comprehensive set of procedures to assess the security requirements.

Keywords

Controlled Unclassified Information; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; nonfederal organizations; nonfederal systems; organization-defined parameter; security assessment; security control; security requirement.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

摘要

保护受控非机密信息(CUI)对于联邦机构至关重要，并可直接影响联邦政府成功履行其基本使命和功能的能力。本出版物为联邦机构提供了推荐的安全要求，用于在信息驻留于非联邦系统和组织时保护CUI的保密性。这些要求适用于处理、存储或传输CUI的非联邦系统组件或为此类组件提供保护。这些安全要求旨在供联邦机构在与非联邦组织建立的合同工具或其他协议中使用。本出版物可与其配套出版物NIST Special publication 800-171A结合使用，后者提供了一套全面的程序来评估这些安全要求。

关键词

受控非机密信息；第13556号行政命令；FIPS出版物199;FIPS
出版物200;FISMA;NIST特别出版物800-53；非联邦组织；非联邦系统；组织定义参数；安全评估；安全控制；安全要求。

计算机系统技术报告

美国国家标准与技术研究院(NIST)的信息技术实验室(ITL)通过为国家测量和标准基础设施提供技术领导，促进美国经济和公共福利。ITL开发测试、测试方法、参考数据、概念验证实现和技术分析，以推进信息技术的发展和高效使用。ITL的职责包括为联邦信息系统中非国家安全相关信息的经济高效的安全和隐私制定管理、行政、技术和物理标准及指南。特别出版物800系列报告了ITL在信息系统安全方面的研究、指南和推广工作，以及其与行业、政府和学术组织的合作活动。

Audience

This publication serves a diverse group of individuals and organizations in the public and private sectors, including:

- Federal agencies responsible for managing and protecting CUI
- Nonfederal organizations responsible for protecting CUI
- Individuals with system development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Individuals with acquisition or procurement responsibilities (e.g., contracting officers)
- Individuals with system, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Individuals with security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, analysts, independent verifiers and validators)

The above roles and responsibilities can be viewed from two perspectives:

- *Federal perspective*: The entity establishing and conveying the security requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with the security requirements set forth in contracts or agreements

受众

本出版物服务于公共和私营部门中多元化的个人和组织群体，包括：

- 负责管理和保护CUI的联邦机构
- 负责保护CUI的非联邦组织
- 承担系统开发生命周期职责的个人(例如，项目经理、任务/业务所有者、信息所有者/管理者、系统设计人员和开发人员、系统/安全工程师、系统集成商)
- 承担采购或采办职责的个人(例如，合同官员)
- 承担系统、安全或风险管理与监督职责的个人(例如，授权官员、首席信息官、首席信息安全官、系统所有者、信息安全管理人)
- 承担安全评估与监控职责的个人(例如，审计员、系统评估员、评估人员、分析师、独立验证与确认人员)

上述角色和职责可以从两个角度来审视：

- 联邦视角：在合同工具或其他类型协议中制定和传达安全要求的实体
- 非联邦视角：响应并遵守合同或协议中规定的安全要求的实体

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

专利披露通知

通知：ITL已要求其使用可能为遵守本出版物的指南或要求所必需的专利主张的持有人向ITL披露此类专利主张。但是，专利持有人没有义务回应ITL的专利征集，ITL也未进行专利检索以确定是否有任何专利可能适用于本出版物。

截至出版之日，在发出关于标识其使用可能为遵守本出版物的指南或要求所必需的专利主张的征集之后，未向ITL标识出任何此类专利主张。

ITL未作出或暗示任何陈述表明在使用本出版物时无需许可即可避免专利侵权。

Table of Contents

1. Introduction 1
1.1. Purpose and Applicability 1
1.2. Organization of This Publication 2
2. The Fundamentals 3
2.1. Security Requirement Assumptions 3
2.2. Security Requirement Development Methodology 3
3. The Security Requirements 6
3.1. Access Control 6
3.2. Awareness and Training 19
3.3. Audit and Accountability 21
3.4. Configuration Management 26
3.5. Identification and Authentication 33
3.6. Incident Response 39
3.7. Maintenance 42
3.8. Media Protection 44
3.9. Personnel Security 48
3.10. Physical Protection 50
3.11. Risk Assessment 53
3.12. Security Assessment and Monitoring 55
3.13. System and Communications Protection 58
3.14. System and Information Integrity 63
3.15. Planning 68
3.16. System and Services Acquisition 70
3.17. Supply Chain Risk Management 72
References 75
Appendix A. Acronyms 83
Appendix B. Glossary 85
Appendix C. Tailoring Criteria 93
Appendix D. Organization-Defined Parameters 106
Appendix E. Change Log 109

目录

1. **引言** 1
1.1. Purpose and Applicability 1
1.2. Organization of This Publication 2
2. **基础** 3
2.1. Security Requirement Assumptions 3
2.2. Security Requirement Development Methodology 3
3. **安全要求** 6
3.1. Access Control 6
3.2. Awareness and Training 19
3.3. Audit and Accountability 21
3.4. Configuration Management 26
3.5. Identification and Authentication 33
3.6. Incident Response 39
3.7. Maintenance 42
3.8. Media Protection 44
3.9. Personnel Security 48
3.10. Physical Protection 50
3.11. Risk Assessment 53
3.12. Security Assessment and Monitoring 55
3.13. System and Communications Protection 58
3.14. System and Information Integrity 63
3.15. Planning 68
3.16. System and Services Acquisition 70
3.17. Supply Chain Risk Management 72
参考文献 75
附录 A.缩略语 83
附录B.术语表 85
附录 C.裁剪准则 93
附录 D.组织定义的参数 106
附录 E.变更日志 109

List of Tables

Table 1. Security Requirement Families 4
Table 2. Security Control Tailoring Criteria 93
Table 3. Access Control (AC) 93
Table 4. Awareness and Training (AT) 94
Table 5. Audit and Accountability (AU) 95
Table 6. Assessment, Authorization, and Monitoring (CA) 95
Table 7. Configuration Management (CM) 96
Table 8. Contingency Planning (CP) 96
Table 9. Identification and Authentication (IA) 97
Table 10. Incident Response (IR) 98
Table 11. Maintenance (MA) 98
Table 12. Media Protection (MP) 99
Table 13. Physical and Environmental Protection (PE) 99
Table 14. Planning (PL) 100
Table 15. Program Management (PM) 100
Table 16. Personnel Security (PS) 101
Table 17. PII Processing and Transparency (PT) 102
Table 18. Risk Assessment (RA) 102
Table 19. System and Services Acquisition (SA) 103
Table 20. System and Communications Protection (SC) 103
Table 21. System and Information Integrity (SI) 104
Table 22. Supply Chain Risk Management (SR) 105
Table 23. Organization-Defined Parameters 106
Table 24. Change Log 110

表格列表

表1. 安全要求族 4
表2. 安全控制裁剪标准 93
表3. 访问控制(AC) 93
表4. 意识与培训(AT) 94
表5. 审计与问责(AU) 95
表6. 评估、授权与监控(CA) 95
表7. 配置管理(CM) 96
表8. 应急计划(CP) 96
表9. 标识与认证(IA) 97
表10. 事件响应(IR) 98
表 11. 维护(MA) 98
表 12. 介质保护(MP) 99
表 13. 物理与环境防护(PE) 99
表 14. 规划(PL) 100
表 15. 项目管理(PM) 100
表16. 人员安全(PS) 101
表17. PII处理与透明度(PT) 102
表18. 风险评估(RA) 102
表 19. 系统与服务获取(SA) 103
表 20. 系统与通信保护(SC) 103
表 21. 系统与信息完整性(SI) 104
表 22. 供应链风险管理(SR) 105
表 23. 组织定义的参数 106
表24. 变更日志 110

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors whose constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura, Isabel Van Wyk, Cristina Ritfeld, Derek Sappington, and Carolyn Schmidt – for their outstanding support in preparing this document for publication. Finally, a special note of thanks goes out to Kelley Dempsey for the initial research and development of the content used in the prototype CUI overlay.

Historical Contributions

The authors also wish to acknowledge the following organizations and individuals for their historic contributions to this publication:

- *Organizations:* National Archives and Records Administration, Department of Defense
- *Individuals:* Carol Bales, Matthew Barrett, Jon Boyens, Devin Casey, Christian Enloe, Gary Guissanie, Peggy Himes, Robert Glenn, Elizabeth Lennon, Vicki Michetti, Dorian Pappas, Karen Quigg, Mark Riddle, Matthew Scholl, Mary Thomas, Murugiah Souppaya, Patricia Toth, and Patrick Viscuso

致谢

作者衷心感谢并赞赏公共和私营部门的个人和组织所做出的重大贡献，他们的建设性意见提高了本出版物的整体质量、全面性和实用性。作者还要感谢NIST的技术编辑和制作人员--Jim Foti、Jeff Brewer、Eduardo Takamura、Isabel Van Wyk、Cristina Ritfeld、Derek Sappington和Carolyn Schmidt--为准备本文件出版所提供的杰出支持。最后，特别感谢Kelley Dempsey对原型CUI覆盖层所用内容的初步研究和开发。

历史贡献

作者还希望感谢以下组织和个人对本出版物的历史性贡献：

- 组织：国家档案和记录管理局、国防部
- 个人：Carol Bales、Matthew Barrett、Jon Boyens、Devin Casey、Christian Enloe、Gary Guissanie、Peggy Himes、Robert Glenn、Elizabeth Lennon、Vicki Michetti、Dorian Pappas、Karen Quigg、Mark Riddle、Matthew Scholl、Mary Thomas、Murugiah Souppaya、Patricia Toth 和 Patrick Viscuso

1. Introduction

Executive Order (EO) 13556 [1] established a government-wide program to standardize the way the executive branch handles Controlled Unclassified Information (CUI).[1] EO 13556 required that the CUI program emphasize openness, transparency, and uniformity of government-wide practices and that the program implementation take place in a manner consistent with Office of Management and Budget (OMB) policies and National Institute of Standards and Technology (NIST) standards and guidelines. As the CUI program Executive Agent, the National Archives and Records Administration (NARA) provides information, guidance, policy, and requirements on handling CUI [4]. This includes approved CUI categories and descriptions, the basis for safeguarding and dissemination controls, and procedures for the use of CUI.[2] The CUI federal regulation [5] provides guidance to federal agencies on the designation, safeguarding, marking, dissemination, decontrolling, and disposition of CUI; establishes self-inspection and oversight requirements; and delineates other facets of the program.

The CUI regulation requires federal agencies that use federal information systems[3] to process, store, or transmit CUI to comply with NIST standards and guidelines. The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal organizations.[4] Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems.[5] To maintain a consistent level of protection, the security requirements for safeguarding CUI in nonfederal systems and organizations must comply with Federal Information Processing Standards (FIPS 199) publication [6] and FIPS 200 [7]. The requirements are derived from the controls in NIST Special Publication (SP) 800-53 [8].

1.1. Purpose and Applicability

This publication provides federal agencies with recommended security requirements[6] for protecting the *confidentiality* of CUI[7] when such information is resident in nonfederal systems and organizations and where there are no specific safeguarding requirements prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI

[1] CUI is any information that a law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under EO 13526 [2], any predecessor or successor order, or the Atomic Energy Act [3] as amended.

[2] Procedures for the use of CUI include marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

[3] A *federal information system* is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. The term *system* is used in this publication to represent people, processes, and technologies involved in the processing, storage, or transmission of CUI. Systems can include operational technology (OT), information technology (IT), Internet of Things (IoT) devices, Industrial IoT (IIoT) devices, specialized systems, cyber-physical systems, embedded systems, and sensors.

[4] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system.

[5] A *nonfederal system* is any system that does not meet the criteria for a federal information system.

[6] The term *security requirement* refers to the protection needs for a system or organization. Security requirements may be derived from laws, Executive Orders, directives, regulations, policies, standards, mission and business needs, or risk assessments.

[7] In accordance with EO 13526 [2] and 32 CFR 2002 [5], the scope of CUI protection is primarily focused on *confidentiality*. However, the security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms support both objectives. Therefore, the security requirements in this publication address the protection of CUI from unauthorized disclosure and modification.

1. 引言

第13556号行政命令(EO)[1]建立了一项政府-wide计划，以标准化行政部门处理受控非机密信息(CUI)的方式。[1] EO 13556要求CUI计划强调政府-wide实践的开放性、透明性和一致性，并且计划的实施方式应与管理和预算办公室(OMB)的政策以及NIST的标准和指南保持一致。作为CUI计划的执行代理，国家档案和记录管理局(NARA)提供有关处理CUI的信息、指南、政策和要求[4]。这包括经批准的CUI类别和描述、保护和传播控制的基础，以及使用CUI的程序。[2] CUI联邦法规[5]为联邦机构提供关于CUI的指定、保护、标记、传播、解除控制和处置的指南；建立自检和监督要求；并描述该计划的其他方面。

CUI法规要求使用联邦信息系统[3]处理、存储或传输CUI的联邦机构遵守NIST标准和指南。当此类信息与非联邦组织共享时，联邦机构保护CUI的责任不会改变。[4]因此，当非联邦组织使用非联邦系统处理、存储或传输CUI时，需要类似级别的保护。[5]为保持一致的保护水平，非联邦系统和组织中保护CUI的安全要求必须符合联邦信息处理标准(FIPS 199)出版物[6]和FIPS 200[7]。这些要求源自NIST特别出版物(SP)800-53[8]中的控制措施。

1.1. 目的与适用范围

本出版物为联邦机构提供了推荐的安全要求[6]，用于在 CUI 驻留于非联邦系统和组织、且 CUI 登记处所列 CUI 类别没有授权法律、法规或政府-wide 政策规定的特定保护要求时，保护 CUI 的保密性[7]

[1] CUI 是指法律、法规或政府-wide 政策要求实施保护或传播控制措施的任何信息，不包括根据 EO 13526[2]、任何前身或后续命令、或经修订的《原子能法》[3]归类为机密的信息。[2] CUI 的使用程序包括标记、保护、传输、传播、重用和处置信息。

[3]联邦信息系统是由行政机构、行政机构的承包商或代表行政机构的另一组织使用或运行的系统。本出版物中使用术语系统来表示处理、存储或传输CUI所涉及的人员、流程和技术。系统可以包括运营技术(OT)、信息技术(IT)、物联网(IoT)设备、工业物联网(IIoT)设备、专用系统、网络物理系统、嵌入式系统和传感器。

[4]非联邦组织是指拥有、运营或维护非联邦系统的任何实体。

[5]非联邦系统是指不符合联邦信息系统标准的任何系统。

[6]术语安全要求是指系统或组织的保护需求。安全要求可源自法律、行政命令、指令、法规、政策、标准、任务和业务需求或风险评估。

[7]根据 EO 13526[2] 和 32 CFR 2002[5],CUI 保护的范围主要侧重于保密性。然而，保密性和完整性的安全目标密切相关，因为许多底层安全机制同时支持这两个目标。因此，本出版物中的安全要求涉及保护 CUI 免遭未经授权的披露和修改。

registry [4]. The requirements do not apply to nonfederal organizations that are collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency.[8]

The security requirements in this publication are *only* applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components.[9] The requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations.

Appropriately scoping requirements is an important factor in determining protection-related investment decisions and managing security risks for nonfederal organizations. If nonfederal organizations designate system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the system components in a separate security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for CUI and avoid increasing the organization's security posture beyond what it requires for protecting its missions, operations, and assets.

1.2. Organization of This Publication

The remainder of this special publication is organized as follows:

- Section 2 describes the assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI, the format of the requirements, and the tailoring criteria applied to the NIST guidelines to obtain the requirements.
- Section 3 lists the security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.

The following sections provide additional information to support the protection of CUI:

- References
- Appendix A: Acronyms
- Appendix B: Glossary
- Appendix C: Tailoring Criteria
- Appendix D: Organization-Defined Parameters
- Appendix E: Change Log

[8] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency must comply with the requirements in FISMA [9].

[9] System *components* include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, and applications.

登记处[4]。这些要求不适用于代表联邦机构收集或维护信息、或代表机构使用或运营系统的非联邦组织。[8]

本出版物中的安全要求仅适用于处理、存储或传输 CUI 的非联邦系统组件或为此类组件提供保护的组件。[9]这些要求旨在供联邦机构在合同工具或这些机构与非联邦组织之间建立的其他协议中使用。

适当界定要求范围是确定保护相关投资决策和管理非联邦组织安全风险的重要因素。如果非联邦组织指定用于处理、存储或传输CUI的系统组件，这些组织可以通过将系统组件隔离在单独的安全域中来限制安全要求的范围。隔离可以通过应用架构和设计概念来实现(例如，实施带防火墙或其他边界保护设备的子网，并使用信息流控制机制)。安全域可以采用物理隔离、逻辑隔离或两者的组合。这种方法可以为CUI提供足够的安全性，并避免将组织的安全态势提高到保护其任务、运营和资产所需之外。

1.2. 本出版物的组织结构

本特别出版物的其余部分组织如下：

- 第 2 节描述了用于制定保护 CUI 保密性安全要求的假设和方法、要求的格式，以及为获得这些要求而对 NIST 指南应用的裁剪标准。
- 第 3 节列出了在非联邦系统和组织中保护 CUI 保密性的安全要求。

以下各节提供支持 CUI 保护的附加信息：

- 参考文献
- 附录 A：缩略语
- 附录B：术语表
- 附录 C：裁剪标准
- 附录D：组织定义的参数
- 附录E：变更日志

[8]代表联邦机构收集或维护信息、或代表机构使用或运营系统的非联邦组织必须遵守 FISMA[9]中的要求。

[9]系统组件包括工作站、服务器、笔记本电脑、智能手机、平板电脑、输入和输出设备、网络组件、操作系统、虚拟机、数据库管理系统和应用程序。

2. The Fundamentals

This section describes the assumptions and methodology used to develop the requirements to protect the confidentiality of CUI in nonfederal systems and organizations. It also includes the tailoring[10] criteria applied to the controls in SP 800-53 [8].

2.1. Security Requirement Assumptions

The security requirements in this publication are based on the following assumptions:

- Federal information designated as CUI has the same value, whether such information resides in a federal or nonfederal system or organization.
- Statutory and regulatory requirements for the protection of CUI are consistent in federal and nonfederal systems and organizations.
- Safeguards implemented to protect CUI are consistent in federal and nonfederal systems and organizations.
- The confidentiality impact value for CUI is no less than *moderate*.[11]
- Nonfederal organizations can directly implement a variety of potential security solutions or use external service providers to satisfy security requirements.

2.2. Security Requirement Development Methodology

Starting with the SP 800-53 controls in the SP 800-53B [12] moderate baseline, the controls are *tailored* to eliminate selected controls or parts of controls that are:

- Primarily the responsibility of the Federal Government,
- Not directly related to protecting the confidentiality of CUI,
- Adequately addressed by other related controls,[12] or
- Not applicable.

SP 800-171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of CUI. The security requirements are organized into 17 families, as illustrated in Table 1. Each family contains the requirements related to the general security topic of the family. Certain families from SP 800-53 are not included due to the tailoring criteria. For example, the PII Processing and Transparency (PT) family is not included because personally identifiable information (PII) is a category of CUI, and therefore, no additional requirements are

[10] *Tailoring* is the process by which control baselines are modified to achieve certain organizational goals and objectives [13].

[11] In accordance with 32 CFR 2002 [5], CUI is categorized at no less than the FIPS 199 [6] moderate confidentiality impact value. However, when federal law, regulation, or government-wide policy establishing the control of CUI specifies controls that differ from those of the moderate control baseline, then the applicable law, regulation, or government-wide policy is followed.

[12] "Adequately addressed by other related controls" means that the protection capability offered by the control is provided by another control in the same or different control family. Using this tailoring option helps to eliminate potential redundancy in requirements without affecting the protection of CUI in nonfederal systems and organizations.

2. 基础知识

本节描述了用于制定在非联邦系统和组织中保护 CUI 保密性要求的假设和方法。它还包括对 SP 800-53[8]中控制措施应用的裁剪[10]标准。

2.1. 安全要求假设

本出版物中的安全要求基于以下假设：

- 被指定为 CUI 的联邦信息具有相同的价值，无论此类信息驻留在联邦还是非联邦系统或组织中。
- 保护 CUI 的法定和监管要求在联邦和非联邦系统和组织中是一致的。
- 为保护 CUI 而实施的安全保障措施在联邦和非联邦系统和组织中是一致的。
- CUI 的保密性影响值不低于中等。[11]
- 非联邦组织可以直接实施各种潜在的安全解决方案，或使用外部服务提供商来满足安全要求。

2.2. 安全要求制定方法

从 SP 800-53B[12]中等基线中的 SP 800-53 控制措施开始，对控制措施进行裁剪，以消除选定的控制措施或控制措施的部分内容，这些内容：

- 主要由联邦政府负责，
- 与保护 CUI 的保密性不直接相关，
- 由其他相关控制措施充分处理，[12]或
- 不适用。

SP 800-171 安全要求代表了保护 CUI 保密性所必需的控制措施的一个子集。这些安全要求被组织为 17 个族，如表 1 所示。每个族包含与该族一般安全主题相关的要求。由于裁剪标准，SP 800-53 中的某些族未被包含。例如，PII 处理与透明度(PT)族未被包含，因为个人可识别信息(PII)是 CUI 的一个类别，因此不需要额外的要求。

[10]裁剪是修改控制基线以实现某些组织目标和目的的过程[13]。

[11]根据 32 CFR 2002[5],CUI 的分类不低于 FIPS 199[6]中等保密性影响值。然而，当确立 CUI 控制的联邦法律、法规或政府-wide 政策规定的控制措施不同于中等控制基线的控制措施时，则遵循适用的法律、法规或政府-wide 政策。

[12] "由其他相关控制措施充分处理"是指该控制措施提供的保护能力由同一或不同控制家族中的另一控制措施提供。使用此裁剪选项有助于消除要求中的潜在冗余，而不影响非联邦系统和组织中 CUI 的保护。

specified for confidentiality protection. The Program Management (PM) family is not included because it is not associated with any control baseline. Finally, the Contingency Planning (CP) family is not included because it addresses availability.[13]

Table 1. Security Requirement Families

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

Organization-defined parameters (ODPs) are included in certain security requirements. ODPs provide flexibility through the use of *assignment* and *selection* operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements.[14] Assignment and selection operations provide the capability to customize the security requirements based on specific protection needs. The determination of ODP values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, the values for the organization-defined parameters become part of the requirement.

ORGANIZATION-DEFINED PARAMETERS

Organization-defined parameters are an important part of a security requirement specification. ODPs provide both the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, operational environments, and risk tolerance. In addition, ODPs support consistent security assessments in determining whether specified security requirements have been satisfied. If a federal agency or a consortium of agencies do not specify a particular value or range of values for an ODP, nonfederal organizations must assign the value or values to complete the security requirement.

A discussion section is included with each requirement. It is derived from the control discussion sections in SP 800-53 and provides additional information to facilitate the implementation and assessment of the requirements. The discussion section is informative, not normative. It is not intended to extend the scope of a requirement or influence the solutions that organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive, and does not reflect the potential options available to organizations. A *references* section provides the source

[13] CP-09 and CP-09(08) are included by exception to ensure the confidentiality of backup information is projected.

[14] NIST does not establish or assign values for ODPs. If ODP values for selected security requirements are not formally established or assigned by a federal agency or a consortium of federal agencies, nonfederal organizations must assign those values to complete the requirements.

为保密性保护而指定。计划管理(PM)家族未包含在内，因为它不与任何控制基线相关联。最后，应急计划(CP)家族未包含在内，因为它涉及可用性。[13]

表 1. 安全要求族

访问控制	维护	安全评估与监控
意识与培训	介质保护	系统与通信保护
审计与问责	人员安全	系统与信息完整性
配置管理	物理保护	规划
标识与身份验证	风险评估	系统与服务获取
事件响应		供应链风险管理

组织定义参数(ODP)包含在某些安全要求中。ODP 通过使用赋值和选择操作提供灵活性，允许联邦机构和非联邦组织为要求中的指定参数指定值。[14]

分配和选择操作提供了自定义以下内容的能力：
基于特定保护需求的安全要求。ODP 值的确定可由法律、行政命令、指令、法规、政策、标准、指南或任务和业务需求来指导和参考。一旦指定，组织定义参数的值就成为要求的一部分。

组织定义参数

组织定义参数是安全要求规范的重要组成部分。ODP 提供了组织所需的灵活性和特异性，以便在其任务、业务功能、运行环境和风险容忍度多样性的情况下，清晰定义其 CUI 安全要求。此外，ODP 支持一致的安全评估，以确定指定的安全要求是否已得到满足。如果联邦机构或机构联合体未为某个 ODP 指定特定值或值范围，非联邦组织必须分配该值或这些值以完成安全要求。

每项要求都包含一个讨论部分。它源自 SP 800-53 中的控制讨论部分，并提供额外信息以促进要求的实施和评估。讨论部分是信息性的，而非规范性的。它不旨在扩展要求的范围或影响组织为满足要求可能采用的解决方案。示例的使用是概念性的，并非穷尽的，也不反映组织可用的潜在选项。参考部分提供了来源。

[13] CP-09和CP-09(08)作为例外包含在内，以确保备份信息的保密性得到保障。

[14] NIST 不建立或分配 ODP 的值。如果选定的安全要求的 ODP 值未由联邦机构或联邦机构联合体正式建立或分配，非联邦组织必须分配这些值以完成要求。

controls[15] from SP 800-53 and a list of NIST Special Publications with additional information on the topic described in the security requirement. The structure and content of a typical security requirement is provided in the example below.

03.13.11 Cryptographic Protection

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. FIPS-validated cryptography is recommended for the protection of CUI.

REFERENCES

Source Control: SC-13

Supporting Publications: FIPS 140-3 [38]

The term *organization* is used in many security requirements, and its meaning depends on context. For example, in a security requirement with an ODP, an organization can refer to either the federal agency or the nonfederal organization establishing the parameter values for the requirement.

Appendix C describes the security control tailoring criteria used to develop the security requirements and the results of the tailoring process. The appendix provides a list of controls from SP 800-53 that support the requirements and the controls that have been eliminated from the moderate baseline in accordance with the tailoring criteria.

ASSESSING SECURITY REQUIREMENTS

SP 800-171A [84] provides a set of procedures to assess the security requirements described in this publication. The assessment procedures are based on the procedures described in SP 800-53A [57].

[15] With few exceptions, the security controls in SP 800-53 are policy-, technology-, and sector-neutral, meaning that the controls focus on the fundamental measures necessary to protect information across the information life cycle.

来自 SP 800-53 的[15]控制措施，以及一份 NIST 特别出版物清单，其中包含有关安全要求所述主题的附加信息。典型安全要求的结构和内容在以下示例中提供。

03.13.11 加密保护

在用于保护 CUI 保密性时，实施以下类型的密码学：[分配：组织定义的密码学类型]。

讨论

密码学按照适用的法律、行政命令、指令、政策、法规、标准和指南实施。建议使用经 FIPS 验证的密码学来保护 CUI。

参考文献

源控制：SC-13

支持性出版物：FIPS 140-3[38]

术语组织在许多安全要求中使用，其含义取决于上下文。例如，在带有 ODP 的安全要求中，组织可以指联邦机构或非联邦组织，即为该要求建立参数值。

附录 C 描述了用于制定安全要求的安全控制裁剪标准以及裁剪过程的结果。该附录提供了来自 SP 800-53 的支持这些要求的控制措施清单，以及根据裁剪标准从中等基线中删除的控制措施。

评估安全要求

SP 800-171A [84] 提供了一套程序，用于评估本出版物中描述的安全要求。评估程序基于 SP 800-53A 中描述的程序。
[57] .

[15]除少数例外，SP 800-53 中的安全控制措施是政策、技术和部门中立的，这意味着这些控制措施侧重于在整个信息生命周期中保护信息所必需的基本措施。

3. The Security Requirements

This section describes 17 families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations. When used in the context of the requirements in Sec. 3, the term *system* is defined to be nonfederal systems or system components that process, store, or transmit CUI or that provide protection for such systems or components. Not all security requirements mention CUI explicitly. However, the requirements are included because they directly affect the protection of CUI during processing, while in storage, and when in transmission between different locations.

Some systems, including specialized systems (e.g., industrial/process control systems, medical devices, computer numerical control machines), may have limitations on the application of certain security requirements. To accommodate such issues, the system security plan — as reflected in requirement 03.15.02 — is used to describe any *enduring exceptions* to the security requirements. Individual, isolated, or temporary deficiencies are managed though plans of action and milestones, as reflected in requirement 03.12.02.

SCOPE AND APPLICABILITY OF SECURITY REQUIREMENTS

The security requirements in this section are only applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components.

3.1. Access Control

03.01.01 Account Management

a. Define the types of system accounts allowed and prohibited.

b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.

c. Specify:

   1. Authorized users of the system,
   2. Group and role membership, and
   3. Access authorizations (i.e., privileges) for each account.

d. Authorize access to the system based on:

   1. A valid access authorization and
   2. Intended system usage.

e. Monitor the use of system accounts.

3. 安全要求

本节描述了用于保护非联邦系统和组织中 CUI 保密性的 17 个安全要求族。当在第 3 节要求的上下文中使用时，术语系统被定义为处理、存储或传输 CUI 的非联邦系统或系统组件，或为此类系统或组件提供保护的系统或系统组件。并非所有安全要求都明确提及 CUI。然而，这些要求被包含在内，因为它们在处理期间、存储期间以及在不同位置之间传输时直接影响 CUI 的保护。

某些系统，包括专用系统(例如，工业/过程控制系统、医疗设备、计算机数控机床)，在应用某些安全要求时可能存在限制。为适应此类问题，系统安全计划--如要求03.15.02所反映--用于描述对安全要求的任何持久性例外。个别、孤立或临时性缺陷通过行动计划和里程碑进行管理，如要求03.12.02所反映。

范围和适用性的安全要求

本节中的安全要求仅适用于处理、存储或传输 CUI或为此类组件提供保护的非联邦系统组件。

3.1. 访问控制

03.01.01 账户管理

a.定义允许和禁止的系统账户类型。b.按照政策、程序、先决条件和标准创建、启用、修改、禁用和删除系统账户。

c. 指定：

   1. 系统的授权用户，
   2. 组和角色成员资格，以及
   3. 每个账户的访问授权(即权限)。

d. 基于以下内容授权对系统的访问：

   1. 有效的访问授权和
   2. 预期系统用途。

e. 监控系统账户的使用情况。

f. Disable system accounts when:

1. The accounts have expired,
2. The accounts have been inactive for [*Assignment: organization-defined time period*],
3. The accounts are no longer associated with a user or individual,
4. The accounts are in violation of organizational policy, or
5. Significant risks associated with individuals are discovered.

g. Notify account managers and designated personnel or roles within:

1. [*Assignment: organization-defined time period*] when accounts are no longer required.
2. [*Assignment: organization-defined time period*] when users are terminated or transferred.
3. [*Assignment: organization-defined time period*] when system usage or the need-to-know changes for an individual.

h. Require that users log out of the system after [*Assignment: organization-defined time period*] of expected inactivity or when [*Assignment: organization-defined circumstances*].

DISCUSSION

This requirement focuses on account management for systems and applications. The definition and enforcement of access authorizations other than those determined by account type (e.g., privileged access, non-privileged access) are addressed in 03.01.02. System account types include individual, group, temporary, system, guest, anonymous, emergency, developer, and service. Users who require administrative privileges on system accounts receive additional scrutiny by personnel responsible for approving such accounts and privileged access. Types of accounts that organizations may prohibit due to increased risk include group, emergency, guest, anonymous, and temporary.

Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of both. Other attributes required for authorizing access include restrictions on the time of day, day of the week, and point of origin. When defining other system account attributes, organizations consider system requirements (e.g., system upgrades, scheduled maintenance) and mission and business requirements (e.g., time zone differences, remote access to facilitate travel requirements).

Users who pose a significant security risk include individuals for whom reliable evidence indicates either the intention to use authorized access to the system to cause harm or that adversaries will cause harm through them. Close coordination

f. 在以下情况下禁用系统账户：

1. 账户已过期，
2. 账户在[分配：组织定义的时间段]内未活动，
3. 这些账户不再与某个用户或个人相关联，
4. 账户违反了组织政策，或
5. 发现与个人相关的重大风险。

g. 在以下范围内通知客户经理和指定人员或角色：

1. [分配：组织定义的时间段]当账户不再需要时。
2. [分配：组织定义的时间段]当用户被解雇或调动时。
3. [分配：组织定义的时间段]当系统使用或个人的知悉需求发生变化时。

h. 要求用户在预期不活动[分配：组织定义的时间段]后或当[分配：组织定义的情况]时注销系统。

讨论

本要求侧重于系统和应用程序的账户管理。除由账户类型确定的访问授权(例如，特权访问、非特权访问)之外的访问授权的定义和执行在

03.01.02中处理。系统账户类型包括个人、组、临时、系统、访客、匿名、紧急、开发者和服务。需要在系统账户上拥有管理权限的用户将受到负责批准此类账户和特权访问的人员的额外审查。组织可能因风险增加而禁止的账户类型包括组、紧急、访客、匿名和临时。

组织可以选择按账户、账户类型或两者的组合来定义访问权限或其他属性。授权访问所需的其他属性包括对一天中的时间、一周中的哪一天以及来源点的限制。在定义其他系统账户属性时，组织应考虑系统需求(例如系统升级、计划维护)以及任务和业务需求(例如时区差异、为便于满足出差需求而进行的远程访问)。

构成重大安全风险的用户包括有可靠证据表明其意图利用对系统的授权访问造成损害，或对手将通过他们造成损害的个人。密切协调

among mission and business owners, system administrators, human resource managers, and legal staff is essential when disabling system accounts for high-risk individuals. Time periods for the notification of organizational personnel or roles may vary.

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by 03.01.10.

REFERENCES

Source Controls: AC-02, AC-02(03), AC-02(05), AC-02(13)

Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

03.01.02 Access Enforcement

Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

DISCUSSION

Access control policies control access between active entities or subjects (i.e., users or system processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. Types of system access include remote access and access to systems that communicate through external networks, such as the internet. Access enforcement mechanisms can also be employed at the application and service levels to provide increased protection for CUI. This recognizes that the system can host many applications and services in support of mission and business functions. Access control policies are defined in 03.15.01.

REFERENCES

Source Control: AC-03

Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

03.01.03 Information Flow Enforcement

Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

任务和业务所有者、系统管理员、人力资源经理和法务人员之间的协调对于禁用高风险个人的系统账户至关重要。通知组织人员或角色的时间段可能有所不同。

不活动注销是基于行为或策略的，要求用户在预期不活动时间超过定义的时间段时采取物理操作来注销。不活动注销的自动执行在03.01.10中处理。

参考文献

源控制：AC-02、AC-02(03)、AC-02(05)、AC-02(13)

支持性出版物：SP 800-46 [14]、SP 800-57-1 [15]、SP 800-57-2 [16]、SP 80057-3 [17]、SP 800-77 [18]、SP 800-113 [19]、SP 800-114 [20]、SP 800-121 [21]、SP 800-162 [22]，SP 800-178 [23]，SP 800-192 [24]，IR 7874 [25]，IR 7966 [26]

03.01.02 访问强制

按照适用的访问控制策略，对CUI和系统资源的逻辑访问执行批准的授权。

讨论

访问控制策略控制组织系统中活动实体或主体(即用户或代表用户行事的系统进程)与被动实体或对象(即设备、文件、记录、域)之间的访问。系统访问的类型包括远程访问以及访问通过外部网络(如互联网)通信的系统。访问执行机制还可以在应用和服务层面采用，以为CUI提供更强的保护。这认识到系统可以承载许多应用和服务以支持任务和业务功能。访问控制策略在03.15.01中定义。

参考文献

源控制：AC-03

支持性出版物：SP 800-46 [14]、SP 800-57-1 [15]、SP 800-57-2 [16]、SP 80057-3 [17]、SP 800-77 [18]、SP 800-113 [19]、SP 800-114 [20]、SP 800-121 [21]、SP 800-162 [22]，SP 800-178 [23]，SP 800-192 [24]，IR 7874 [25]，IR 7966 [26]

03.01.03 信息流强制

执行批准的授权，以控制CUI在系统内以及连接系统之间的流动。

DISCUSSION

Information flow control regulates where CUI can transit within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include keeping CUI from being transmitted in the clear to the internet, blocking external communications traffic that claims to be sourced from within the organization, restricting requests to the internet that are not from the internal web proxy server, and limiting CUI transfers between organizations based on data structures and content.

Transferring CUI between organizations may require an agreement that specifies how the information flow is enforced (see 03.12.05). Transferring CUI between systems that represent different security domains with different security policies introduces the risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes prohibiting CUI transfers between interconnected systems (i.e., allowing information access only), employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of CUI between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., encrypted tunnels, routers, gateways, and firewalls) that use rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

REFERENCES

Source Control: AC-04

Supporting Publications: SP 800-160-1 [11], SP 800-162 [22], SP 800-178 [23]

03.01.04 Separation of Duties

a. Identify the duties of individuals requiring separation.

b. Define system access authorizations to support separation of duties.

讨论

信息流控制规范CUI可以在系统内以及系统之间传输的位置(与之相对的是谁被允许访问该信息)，并且不考虑对该信息的后续访问。流控制限制包括防止CUI以明文形式传输到互联网、阻止声称源自组织内部的外部通信流量、限制并非来自内部Web代理服务器的互联网请求，以及基于数据结构和内容限制组织之间的CUI传输。

在组织之间传输CUI可能需要一项协议，规定信息流如何被执行(见03.12.05)。在代表具有不同安全策略的不同安全域的系统之间传输CUI会带来此类传输违反一个或多个域安全策略的风险。在此类情况下，信息所有者或管理者在互连系统之间的指定策略执行点提供指导。组织考虑在需要执行特定安全策略时强制实施特定的架构解决方案。执行包括禁止互连系统之间的CUI传输(即仅允许信息访问)、采用硬件机制执行单向信息流，以及实施可信的重新分级机制以重新分配安全属性和安全标签。

组织通常使用信息流控制策略和执行机制来控制CUI在系统内以及互连系统之间在指定来源和目的地(例如网络、个人和设备)之间的流动。流控制基于信息或信息路径的特征。执行发生在边界保护设备(例如加密隧道、路由器、网关和防火墙)中，这些设备使用规则集或建立配置设置，以限制系统服务、提供基于报头信息的数据包过滤能力，或提供基于消息内容的消息过滤能力(例如实施关键字搜索或使用文档特征)。组织还考虑对信息流执行至关重要的过滤和检查机制(即硬件、固件和软件组件)的可信度。

参考文献

源控制：AC-04

支持性出版物：SP 800-160-1[11]、SP 800-162[22]、SP 800-178[23]

03.01.04 **职责分离**

a. 确定需要离职人员的职责。

b. 定义系统访问授权以支持职责分离。

DISCUSSION

Separation of duties addresses the potential for abuse of authorized privileges and reduces the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and support functions among different individuals or roles, conducting system support functions with different individuals or roles (e.g., quality assurance, configuration management, network security, system management, assessments, and programming), and ensuring that personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of their systems and system components when developing policies on separation of duties. This requirement is enforced by 03.01.02.

REFERENCES

Source Control: AC-05

Supporting Publications: SP 800-162 [22], SP 800-178 [23]

03.01.05 Least Privilege

a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.

b. Authorize access to [*Assignment: organization-defined security functions*] and [*Assignment: organization-defined security-relevant information*].

c. Review the privileges assigned to roles or classes of users [*Assignment: organization-defined frequency*] to validate the need for such privileges.

d. Reassign or remove privileges, as necessary.

DISCUSSION

Organizations employ the principle of least privilege for specific duties and authorized access for users and system processes. Least privilege is applied to the development, implementation, and operation of the system. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Security functions include establishing system accounts and assigning privileges, installing software, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information. Security-relevant information includes threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, security architecture, cryptographic key management information, access control lists, and audit information.

讨论

职责分离旨在应对授权权限被滥用的可能性，并降低无共谋情况下恶意活动的风险。职责分离包括将任务功能和支持功能分配给不同个人或角色，由不同个人或角色执行系统支持功能(例如质量保证、配置管理、网络安全、系统管理、评估和编程)，并确保管理访问控制功能的人员不同时管理审计功能。由于职责分离违规可能跨越系统和应用领域，组织在制定职责分离政策时应考虑其系统和系统组件的整体。本要求由03.01.02强制执行。

参考文献

源控制：AC-05

支持性出版物：SP 800-162[22],SP 800-178[23]

03.01.05 最小权限

a. 仅允许用户(或代表用户行事的进程)进行完成所分配组织任务所必需的授权系统访问。

b. 授权访问[分配：组织定义的安全功能]和[分配：组织定义的安全相关信息]。

c. [分配：组织定义的频率]审查分配给角色或用户类别的权限，以验证此类权限的必要性。

d. 根据需要重新分配或移除权限。

讨论

组织对特定职责和用户及系统进程的授权访问采用最小权限原则。最小权限应用于系统的开发、实施和运行。组织考虑创建额外的进程、角色和系统账户以实现最小权限。安全功能包括建立系统账户和分配权限、安装软件、配置访问授权、配置要审计事件的设置、建立脆弱性扫描参数、建立入侵检测参数以及管理审计信息。安全相关信息包括威胁和脆弱性信息、路由器或防火墙的过滤规则、安全服务的配置参数、安全架构、密码密钥管理信息、访问控制列表和审计信息。

REFERENCES

Source Controls: AC-06, AC-06(01), AC-06(07), AU-09(04)

Supporting Publications: None

03.01.06 Least Privilege – Privileged Accounts

a. Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or roles*].

b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.

DISCUSSION

Privileged accounts refer to accounts that are granted elevated privileges to access resources (including security functions or security-relevant information) that are otherwise restricted for non-privileged accounts. These accounts are typically described as system administrator or super user accounts. For example, a privileged account is often required in order to perform privileged functions such as executing commands that could modify system behavior. Restricting privileged accounts to specific personnel or roles ensures that only those authorized users can access and manipulate security functions or security-relevant information. Requiring the use of non-privileged accounts when such access is not needed can limit unauthorized access to and manipulation of security functions or security-relevant information.

REFERENCES

Source Controls: AC-06(02), AC-06(05)

Supporting Publications: None

03.01.07 Least Privilege – Privileged Functions

a. Prevent non-privileged users from executing privileged functions.

b. Log the execution of privileged functions.

DISCUSSION

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, changing system configuration settings, or administering cryptographic key management activities. Non-privileged users do not possess the authorizations to execute privileged functions. Bypassing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. This requirement represents a condition achieved by the definition of authorized privileges in 03.01.01 and privilege enforcement in 03.01.02.

参考文献

源控制：AC-06、AC-06(01)、AC-06(07)、AU-09(04)支
持出版物：无

03.01.06 最小权限 - 特权账户

a. 将系统上的特权账户限制为[分配：组织定义的人员或角色]。

b. 要求拥有特权账户的用户(或角色)在访问非安全功能或非安全信息时使用非特权账户。

讨论

特权账户是指被授予提升权限以访问非特权账户通常受限的资源(包括安全功能或安全相关信息)的账户。这些账户通常被描述为系统管理员或超级用户账户。例如，通常需要特权账户来执行特权功能，例如执行可能修改系统行为的命令。将特权账户限制为特定人员或角色可确保只有那些授权用户才能访问和操作安全功能或安全相关信息。在不需要此类访问时要求使用非特权账户，可以限制对安全功能或安全相关信息的未授权访问和操作。

参考文献

源控制：AC-06(02), AC-06(05)

支持性出版物：无

03.01.07 最小权限 - 特权功能

a. 防止非特权用户执行特权功能。

b. 记录特权功能的执行情况。

讨论

特权功能包括建立系统账户、执行系统完整性检查、执行补丁操作、更改系统配置设置或管理密码密钥管理活动。非特权用户不具备执行特权功能的授权。绕过入侵检测和防御机制或恶意代码保护机制是需要保护免受非特权用户侵害的特权功能的示例。本要求代表通过03.01.01中授权权限的定义和03.01.02中权限执行所达到的条件。

The misuse of privileged functions — whether intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts — is a serious and ongoing concern that can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse and mitigate risks from advanced persistent threats and insider threats.

REFERENCES

Source Controls: AC-06(09), AC-06(10)

Supporting Publications: None

03.01.08 Unsuccessful Logon Attempts

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*].

b. Automatically [*Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action*] when the maximum number of unsuccessful attempts is exceeded.

DISCUSSION

Due to the potential for denial of service, automatic system lockouts are in most cases, temporary and automatically release after a predetermined time period established by the organization (i.e., using a delay algorithm). Organizations may employ different delay algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful system logon attempts may be implemented at the system and application levels.

Organization-defined actions that may be taken include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of a full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles, such as location, time of day, IP address, device, or Media Access Control (MAC) address.

REFERENCES

Source Control: AC-07

Supporting Publications: SP 800-63-3 [27], SP 800-124 [28]

特权功能的滥用--无论是授权用户有意或无意，还是已攻破系统账户的未授权外部实体--都是一个严重且持续存在的问题，可能对组织产生重大不利影响。记录特权功能的使用是检测此类滥用并缓解来自高级持续威胁和内部威胁的风险的一种方法。

参考文献

源控制：AC-06(09)、AC-06(10)

支持性出版物：无

03.01.08 登录尝试失败

a. 在[分配：组织定义的时间段]内，对用户连续无效登录尝试强制执行[分配：组织定义的数量]次限制。

b. 当超过最大失败尝试次数时，自动[选择*(一项或多项)*：将账户或节点锁定[分配：组织定义的时间段] ；将账户或节点锁定直至管理员释放；延迟下一次登录提示；通知系统管理员；采取其他措施]。

讨论

由于可能存在拒绝服务，自动系统锁定在大多数情况下是临时的，并在组织设定的预定时间段后自动释放(即使用延迟算法)。组织可以根据各组件的能力为不同的系统组件采用不同的延迟算法。对不成功系统登录尝试的响应可以在系统和应用程序级别实施。

组织定义的可以采取的措施包括提示用户在用户名和密码之外回答一个秘密问题、调用具有有限用户能力的锁定模式(而不是完全锁定)、允许用户仅从指定的互联网协议(IP)地址登录、要求CAPTCHA以防止自动化攻击，或应用用户配置文件，如位置、一天中的时间、IP地址、设备或媒体访问控制(MAC)地址。

参考文献

源控制：AC-07

支持性出版物：SP 800-63-3[27]、SP 800-124[28]

03.01.09 System Use Notification

Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.

DISCUSSION

System use notifications can be implemented using messages or warning banners. The messages or warning banners are displayed before individuals log in to a system that processes, stores, or transmits CUI. System use notifications are used for access via logon interfaces with human users and are not required when human interfaces do not exist. Organizations consider whether a secondary use notification is needed to access applications or other system resources after the initial network logon. Posters or other printed materials may be used in lieu of an automated system message. This requirement is related to 03.15.03.

REFERENCES

Source Control: AC-08

Supporting Publications: None

03.01.10 Device Lock

a. Prevent access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*].

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

DISCUSSION

Device locks are temporary actions taken to prevent access to the system when users depart from the immediate vicinity of the system but do not want to log out due to the temporary nature of their absences. Device locks can be implemented at the operating system level or application level. User-initiated device locking is behavior- or policy-based and requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of the system (e.g., when organizations require users to log out at the end of workdays). Publicly viewable images can include static or dynamic images, such as patterns used with screen savers, solid colors, photographic images, a clock, a battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

03.01.09 系统使用通知

在授予系统访问权限之前，显示带有符合适用CUI规则的隐私和安全通知的系统使用通知消息。

讨论

系统使用通知可以使用消息或警告横幅来实现。消息或警告横幅在个人登录处理、存储或传输CUI的系统之前显示。系统使用通知用于通过具有人类用户的登录界面进行访问，当不存在人类界面时不需要。组织考虑在初始网络登录后访问应用程序或其他系统资源是否需要二次使用通知。海报或其他印刷材料可以代替自动化系统消息使用。本要求与03.15.03相关。

参考文献

源控制：AC-08

支持性出版物：无

03.01.10 设备锁定

a. 通过[选择*(一项或多项)*：在[分配：组织定义的时间段] 不活动后启动设备锁定；要求用户在离开系统无人看管之前启动设备锁定]来防止对系统的访问。

b. 保持设备锁定，直到用户使用既定的身份验证和身份验证程序重新建立访问。

c. 通过设备锁定，用可公开查看的图像隐藏先前在显示器上可见的信息。

讨论

设备锁定是为防止用户在离开系统附近区域但因其离开是临时性的而不愿注销时访问系统而采取的临时措施。设备锁定可在操作系统层面或应用层面实现。用户发起的设备锁定基于行为或策略，要求用户采取物理操作来启动设备锁定。设备锁定不能替代注销系统(例如，当组织要求用户在工作日结束时注销时)。公开可见的图像可包括静态或动态图像，例如屏幕保护程序中使用的图案、纯色、照片图像、时钟、电池寿命指示器或空白屏幕，但前提是不显示受控非机密信息。

REFERENCES

Source Controls: AC-11, AC-11(01)

Supporting Publications: None

03.01.11 Session Termination

Terminate a user session automatically after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

DISCUSSION

This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network) in 03.13.09. A logical session is initiated whenever a user (or processes acting on behalf of a user) accesses a system. Logical sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination ends all system processes associated with a user's logical session except those processes that are created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic session termination can include organization-defined periods of user inactivity, time-of-day restrictions on system use, and targeted responses to certain types of incidents.

REFERENCES

Source Control: AC-12

Supporting Publications: None

03.01.12 Remote Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

b. Authorize each type of remote system access prior to establishing such connections.

c. Route remote access to the system through authorized and managed access control points.

d. Authorize the remote execution of privileged commands and remote access to security-relevant information.

DISCUSSION

Remote access is access to systems (or processes acting on behalf of users) that communicate through external networks, such as the internet. Monitoring and controlling remote access methods allows organizations to detect attacks and

参考文献

源控制：AC-11、AC-11(01)

支持性出版物：无

03.01.11 会话终止

在[分配：组织定义的需断开会话的条件或触发事件]后自动终止用户会话。

讨论

本要求涉及终止用户发起的逻辑会话，与03.13.09中终止与通信会话相关的网络连接(即断开网络连接)不同。当用户(或代表用户行事的进程)访问系统时，即启动逻辑会话。逻辑会话可在不终止网络会话的情况下终止(从而终止用户访问)。会话终止会结束与用户逻辑会话相关的所有系统进程，但用户(即会话所有者)创建的、在会话终止后继续运行的进程除外。需要自动会话终止的条件或触发事件可包括组织定义的用户不活动时间段、系统使用的时间限制以及对某些类型事件的针对性响应。

参考文献

源控制：AC-12

支持性出版物：无

03.01.12 远程访问

a. 为每种允许的远程系统访问建立使用限制、配置要求和连接要求。

b. 在建立此类连接之前，授权每种类型的远程系统访问。

c. 通过经授权和管理的访问控制点路由对系统的远程访问。

d. 授权特权命令的远程执行和对安全相关信息的远程访问。

讨论

远程访问是指通过外部网络(如互联网)通信的系统(或代表用户执行的进程)的访问。监控和控制远程访问方法使组织能够检测攻击并

ensure compliance with remote access policies. Routing remote access through managed access control points enhances explicit control over such connections and reduces susceptibility to unauthorized access to the system, which could result in the unauthorized disclosure of CUI.

Remote access to the system represents a significant potential vulnerability that can be exploited by adversaries. Restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and its susceptibility to threats by adversaries. A privileged command is a human-initiated command executed on a system that involves the control, monitoring, or administration of the system, including security functions and security-relevant information. Security-relevant information is information that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions.

REFERENCES

Source Controls: AC-17, AC-17(03), AC-17(04)

Supporting Publications: SP 800-46 [14], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], IR 7966 [26]

03.01.13 Withdrawn

Addressed by 03.13.08.

03.01.14 Withdrawn

Incorporated into 03.01.12.

03.01.15 Withdrawn

Incorporated into 03.01.12.

03.01.16 Wireless Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.

b. Authorize each type of wireless access to the system prior to establishing such connections.

c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.

确保符合远程访问策略。通过受管理的访问控制点路由远程访问可增强对此类连接的明确控制，并降低系统遭受未经授权访问的可能性，从而可能导致CUI的未经授权披露。

对系统的远程访问是一个重大的潜在脆弱性，可被对手利用。限制通过远程访问执行特权命令和访问安全相关信息，可减少组织的暴露面及其受对手威胁的 susceptibility。特权命令是在系统上执行的人工发起命令，涉及系统的控制、监控或管理，包括安全功能和安全相关信息。安全相关信息是指可能以导致无法执行系统安全策略或无法维持代码和数据隔离的方式影响安全功能运行或安全服务提供的信息。特权命令使个人能够执行敏感、安全关键或安全相关的系统功能。

参考文献

源控制：AC-17、AC-17(03)、AC-17(04)

支持性出版物：SP 800-46[14]、SP 800-77[18]、SP 800-113[19]、SP 800-114 [20]、SP 800-121 [21]、IR 7966 [26]

03.01.13 **已撤回**

由03.13.08涵盖。

03.01.14 **已撤回**

已纳入03.01.12。

03.01.15 **已撤回**

已纳入03.01.12。

03.01.16 **无线访问**

a. 为每种类型的无线系统访问建立使用限制、配置要求和连接要求。

b. 在建立此类连接之前，授权每种类型的无线系统访问。

c. 在发放和部署之前，禁用不打算使用的无线网络功能。

d. Protect wireless access to the system using authentication and encryption.

DISCUSSION

Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. Establishing usage restrictions, configuration requirements, and connection requirements for wireless access to the system provides criteria to support access authorization decisions. These restrictions and requirements reduce susceptibility to unauthorized system access through wireless technologies. Wireless networks use authentication protocols that provide credential protection and mutual authentication. Organizations authenticate individuals and devices to protect wireless access to the system. Special attention is given to the variety of devices with potential wireless access to the system, including small form factor mobile devices (e.g., smart phones, tablets, smart watches). Wireless networking capabilities that are embedded within system components represent a potential vulnerability that can be exploited by adversaries. Strong authentication of users and devices, strong encryption, and disabling wireless capabilities that are not needed for essential mission or business functions can reduce susceptibility to threats by adversaries involving wireless technologies.

REFERENCES

Source Controls: AC-18, AC-18(01), AC-18(03)

Supporting Publications: SP 800-94 [29], SP 800-97 [30], SP 800-124 [28]

03.01.17 Withdrawn

Incorporated into 03.01.16.

03.01.18 Access Control for Mobile Devices

a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.

b. Authorize the connection of mobile devices to the system.

c. Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.

DISCUSSION

A mobile device is a computing device with a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable, or removable data storage; and includes a self-contained power source. Mobile device functionality may include on-board sensors that allow the device to capture information, voice communication capabilities, and/or built-in features for synchronizing local data with remote locations. Examples

d. 使用身份验证和加密保护对系统的无线访问。

讨论

无线网络能力是一个重大的潜在脆弱性，可被对手利用。为对系统的无线访问建立使用限制、配置要求和连接要求，可为访问授权决策提供依据。这些限制和要求可降低通过无线技术未经授权访问系统的 susceptibility。无线网络使用提供凭据保护和双向身份验证的身份验证协议。组织对个人和设备进行身份验证，以保护对系统的无线访问。应特别关注可能对系统进行无线访问的各种设备，包括小型移动设备(例如智能手机、平板电脑、智能手表)。嵌入系统组件中的无线网络能力是一个可被对手利用的潜在脆弱性。对用户和设备进行强身份验证、强加密以及禁用基本任务或业务功能不需要的无线能力，可降低受涉及无线技术的对手威胁的 susceptibility。

参考文献

源控制：AC-18、AC-18(01)、AC-18(03)

支持性出版物：SP 800-94[29]、SP 800-97[30]、SP 800-124[28]

03.01.17 已撤回

已纳入03.01.16。

03.01.18 移动设备的访问控制

a. 为移动设备建立使用限制、配置要求和连接要求。

b. 授权移动设备连接到系统。

c. 实施全设备或基于容器的加密，以保护移动设备上CUI的保密性。

讨论

移动设备是一种外形小巧、可由单人携带的计算设备；设计为无需物理连接即可运行；具有本地、不可移除或可移除的数据存储；并包含自备电源。移动设备功能可能包括允许设备捕获信息的板载传感器、语音通信能力，和/或用于将本地数据与远程位置同步的内置功能。示例

include smart phones, smart watches, and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capabilities of mobile devices may be comparable to or a subset of notebook or desktop systems, depending on the nature and intended purpose of the device. Some organizations may consider notebook computers to be mobile devices. The protection and control of mobile devices are behavior- or policy-based and require users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which the organization provides physical or procedural controls to meet the requirements established for protecting CUI.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions, configuration requirements, and connection requirements for mobile devices include configuration management, device identification and authentication, implementing mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting operating system and possibly other software integrity checks, and disabling unnecessary hardware. On mobile devices, secure containers provide software-based data isolation designed to segment enterprise applications and information from personal apps and data. Containers may present multiple user interfaces, one of the most common being a mobile application that acts as a portal to a suite of business productivity apps, such as email, contacts, and calendar. Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices.

REFERENCES

Source Controls: AC-19, AC-19(05)

Supporting Publications: SP 800-46 [14], SP 800-114 [31], SP 800-124 [28]

03.01.19 Withdrawn

Incorporated into 03.01.18.

03.01.20 Use of External Systems

a. Prohibit the use of external systems unless the systems are specifically authorized.

b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [*Assignment: organization-defined security requirements*].

c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:

包括智能手机、智能手表和平板电脑。移动设备通常与单个个人相关联。根据设备的性质和预期用途，移动设备的处理、存储和传输能力可能与笔记本电脑或台式系统相当，或是其子集。一些组织可能将笔记本电脑视为移动设备。移动设备的保护和控制基于行为或策略，要求用户在受控区域外采取物理操作来保护和控制此类设备。受控区域是组织提供物理或程序控制以满足为保护 CUI 所确立要求的空间。

由于具有不同特性和能力的移动设备种类繁多，组织对不同类型的此类设备可能施加不同的限制。移动设备的使用限制、配置要求和连接要求包括配置管理、设备标识与身份验证、实施强制性防护软件、扫描设备以检测恶意代码、更新病毒防护软件、扫描关键软件更新和补丁、执行操作系统以及可能的其他软件完整性检查，以及禁用不必要的硬件。在移动设备上，安全容器提供基于软件的数据隔离，旨在将企业应用和信息与个人应用和数据分隔开。容器可能呈现多个用户界面，其中最常见的是作为一组业务生产力应用(如电子邮件、联系人和日历)门户的移动应用。组织可以采用全设备加密或基于容器的加密来保护移动设备上 CUI 的保密性。

参考文献

源控制：AC-19、AC-19(05)

支持性出版物：SP 800-46[14]、SP 800-114[31]、SP 800-124[28]

03.01.19 已撤回

已纳入03.01.18。

03.01.20 外部系统的使用

a. 禁止使用外部系统，除非系统被特别授权。

b. 在允许授权个人使用或访问外部系统之前，建立以下需在外部系统上满足的安全要求：[赋值：组织定义的安全要求]。

c. 仅在以下条件满足后，才允许授权个人使用外部系统访问组织系统或处理、存储或传输CUI:

1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and
2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

DISCUSSION

External systems are systems that are used by but are not part of the organization. These systems include personally owned systems, system components, or devices; privately owned computing and communication devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; and systems managed by contractors. Organizations have the option to prohibit the use of any type of external system or specified types of external systems (e.g., prohibit the use of external systems that are not organizationally owned). Terms and conditions are consistent with the trust relationships established with the entities that own, operate, or maintain external systems and include descriptions of shared responsibilities.

Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to the organizational system and over whom organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals may vary depending on the trust relationships between organizations. Organizations need assurance that external systems satisfy the necessary security requirements so as not to compromise, damage, or harm the system. This requirement is related to 03.16.03.

REFERENCES

Source Controls: AC-20, AC-20(01), AC-20(02)

Supporting Publications: None

03.01.21 Withdrawn

Incorporated into 03.01.20.

03.01.22 Publicly Accessible Content

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

b. Review the content on publicly accessible systems for CUI and remove such information, if discovered.

1. 验证外部系统上的安全要求(如组织系统安全计划中所规定)已得到满足，并且
2. 保留与托管外部系统的组织实体的已批准系统连接或处理协议。

d. 限制授权个人在外部系统上使用组织控制的便携式存储设备。

讨论

外部系统是由组织使用但不属于组织所有的系统。这些系统包括个人拥有的系统、系统组件或设备；商业或公共设施中私人拥有的计算和通信设备；非联邦组织拥有或控制的系统；以及由承包商管理的系统。组织可以选择禁止使用任何类型的外部系统或指定类型的外部系统(例如，禁止使用非组织所有的外部系统)。条款和条件与同拥有、运营或维护外部系统的实体建立的信任关系一致，并包括对共同责任的描述。

授权个人包括组织人员、承包商或其他经授权访问组织系统且组织有权对其施加有关系统访问的特定行为规则的个人。组织对授权个人施加的限制可能因组织之间的信任关系而异。组织需要确保外部系统满足必要的安全要求，以免危及、损坏或损害系统。本要求与03.16.03相关。

参考文献

源控制：AC-20、AC-20(01)、AC-20(02)支持性出版物：无

03.01.21 已撤回

纳入03.01.20。

03.01.22 公开可访问内容

a. 培训授权个人，确保可公开访问的信息不包含CUI。

b. 审查可公开访问系统上的内容是否包含CUI，如发现此类信息则予以移除。

DISCUSSION

In accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including CUI.

REFERENCES

Source Control: AC-22

Supporting Publications: None

3.2. Awareness and Training

03.02.01 Literacy Training and Awareness

a. Provide security literacy training to system users:

   1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter,
   2. When required by system changes or following [*Assignment: organization-defined events*], and
   3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.

b. Update security literacy training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

DISCUSSION

Organizations provide basic and advanced levels of security literacy training to system users (including managers, senior executives, system administrators, and contractors) and measures to test the knowledge level of users. Organizations determine the content of literacy training based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and the actions required of users to maintain security and respond to incidents. The content also addresses the need for operations security and the handling of CUI.

Security awareness techniques include displaying posters, offering supplies inscribed with security reminders, generating email advisories or notices from organizational officials, displaying logon screen messages, and conducting awareness events using podcasts, videos, and webinars. Security literacy training is conducted at a frequency consistent with applicable laws, directives, regulations, and policies. Updating literacy training content on a regular basis ensures that the content remains relevant. Events that may precipitate an update to literacy training content include

讨论

根据适用法律、行政命令、指令、政策、法规、标准和指南，公众无权访问非公开信息，包括CUI。

参考文献

源控制：AC-22

支持性出版物：无

3.2. 意识与培训

03.02.01 素养培训与意识

a. 向系统用户提供安全素养培训：

   1. 作为新用户初始培训的一部分，以及此后[赋值：组织定义的频率],
   2. 当系统变更要求时或发生[赋值：组织定义的事件]之后，以及
   3. 关于识别和报告内部威胁、社会工程和社会挖掘的指标。

b. 按[赋值：组织定义的频率]及发生[赋值：组织定义的事件]之后更新安全素养培训内容。

讨论

组织为系统用户(包括管理人员、高级主管、系统管理员和承包商)提供基础级和高级别的安全素养培训，以及测试用户知识水平的措施。组织根据具体的组织要求、人员经授权访问的系统以及工作环境(例如远程办公)确定素养培训的内容。内容包括对安全需求的理解以及用户为维护安全和响应事件所需采取的行动。内容还涉及操作安全的需要和 CUI 的处理。

安全意识技术包括展示海报、提供印有安全提醒的用品、生成组织官员的电子邮件建议或通知、显示登录屏幕消息，以及使用播客、视频和网络研讨会开展意识活动。安全素养培训按照与适用法律、指令、法规和政策一致的频率进行。定期更新素养培训内容可确保内容保持相关性。可能促使更新素养培训内容的事件包括

assessment or audit findings, security incidents or breaches, or changes in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

Potential indicators and possible precursors of insider threats include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; sexual harassment or bullying of fellow employees; workplace violence; and other serious violations of the policies, procedures, rules, directives, or practices of organizations. Organizations may consider tailoring insider threat awareness topics to roles (e.g., training for managers may be focused on specific changes in the behavior of team members, while training for employees may be focused on more general observations).

Social engineering is an attempt to deceive an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, threadjacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Security literacy training includes how to communicate employee and management concerns regarding potential indicators of insider threat and potential and actual instances of social engineering and data mining through appropriate organizational channels in accordance with established policies and procedures.

REFERENCES

Source Controls: AT-02, AT-02(02), AT-02(03)

Supporting Publications: SP 800-50 [32], SP 800-160-2 [10]

03.02.02 Role-Based Training

a. Provide role-based security training to organizational personnel:
   1. Before authorizing access to the system or CUI, before performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter
   2. When required by system changes or following [*Assignment: organization-defined events*].

b. Update role-based training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

DISCUSSION

Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of the systems to which personnel have authorized access. In addition,

评估或审计发现、安全事件或违规，或适用法律、行政命令、指令、法规、政策、标准和指南的变更。

内部威胁的潜在指标和可能前兆包括以下行为：过度且长期的工作不满；试图获取工作绩效所不需要的信息；无法解释的财务资源获取；对同事的性骚扰或欺凌；工作场所暴力；以及其他严重违反组织政策、程序、规则、指令或做法的行为。组织可以考虑根据角色定制内部威胁意识主题(例如，针对管理人员的培训可能侧重于团队成员行为的特定变化，而针对员工的培训可能侧重于更一般的观察)。

社会工程是试图欺骗个人泄露信息或采取可用于破坏、危及或以其他方式对系统产生不利影响的行动。社会工程包括网络钓鱼、借口托词、冒充、诱饵、交换条件、话题劫持、社交媒体利用和尾随。社会挖掘是试图收集可能用于支持未来攻击的组织信息。安全素养培训包括如何按照既定政策和程序，通过适当的组织渠道，就内部威胁的潜在指标以及社会工程和数据挖掘的潜在和实际实例，传达员工和管理层的关切。

参考文献

来源控制：AT-02、AT-02(02)、AT-02(03)

支持性出版物：SP 800-50[32]、SP 800-160-2[10]

03.02.02 基于角色的培训

a. 为组织人员提供基于角色的安全培训：
   1. 在授权访问系统或CUI之前、在履行分配职责之前，以及[分配：组织定义的频率]之后
   2. 当系统变更要求时或发生[分配：组织定义的事件]之后。

b. 更新基于角色的培训内容[分配：组织定义的频率]以及在[分配：组织定义的事件]之后。

讨论

组织根据个人的分配职责、角色和责任，以及人员被授权访问的系统的安全要求，确定安全培训的内容和频率。此外，

organizations provide system developers, enterprise architects, security architects, software developers, systems integrators, acquisition/procurement officials, system and network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and personnel with access to system-level software with security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities that cover physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

REFERENCES

Source Control: AT-03

Supporting Publications: SP 800-161 [33], SP 800-181 [34]

03.02.03 Withdrawn

Incorporated into 03.02.01.

3.3. Audit and Accountability

03.03.01 Event Logging

a. Specify the following event types selected for logging within the system: [*Assignment: organization-defined event types*].

b. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

DISCUSSION

An event is any observable occurrence in a system, including unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed. This includes events that are relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, the execution of privileged functions, failed logons or accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the system monitoring and auditing that are appropriate for each of the security requirements. When defining event types, organizations consider the logging necessary to cover related events, such as the

组织为系统开发者、企业架构师、安全架构师、软件开发人员、系统集成商、采购/采办官员、系统和网络管理员、执行配置管理和审计活动的人员、执行独立验证和确认的人员、安全评估人员以及有权访问系统级软件的人员提供专门针对其分配职责定制的安全相关技术培训。

全面的基于角色的培训涉及管理、运营和技术角色与职责，涵盖物理、人员和技术控制。此类培训可包括为所定义安全角色制定的政策、程序、工具和工件。组织还提供必要培训，使个人能够在组织信息安全计划的背景下履行与运营和供应链安全相关的职责。

参考文献

源控制：AT-03

支持性出版物：SP 800-161[33]、SP 800-181[34]

03.02.03 已撤回

已纳入03.02.01。

3.3. 审计与问责

03.03.01 事件日志记录

a. 指定以下选定用于系统内日志记录的事件类型：[分配：组织定义的事件类型]。

b. 审查并更新选定用于日志记录的事件类型[分配：组织定义的频率]。

讨论

事件是系统中任何可观察到的发生，包括非法或未经授权的系统活动。组织确定需要日志记录功能的 event 类型。这包括与系统及这些系统运行环境的安全相关的事件，以满足特定和持续的审计需求。事件类型可以包括密码更改、特权功能的执行、与系统相关的登录或访问失败、管理特权使用或第三方凭据使用。在确定需要日志记录的事件类型时，组织考虑适合每项安全要求的系统监控和审计。在定义事件类型时，组织考虑覆盖相关事件所需的日志记录，例如

steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access — both successful and unsuccessful — but only activate that capability under specific circumstances due to the potential burden on system performance. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types are necessary to ensure that the current set of event types remains relevant.

REFERENCES

Source Control: AU-02

Supporting Publications: SP 800-92 [35]

03.03.02 Audit Record Content

a. Include the following content in audit records:
   1. What type of event occurred
   2. When the event occurred
   3. Where the event occurred
   4. Source of the event
   5. Outcome of the event
   6. Identity of the individuals, subjects, objects, or entities associated with the event

b. Provide additional information for audit records as needed.

DISCUSSION

Audit record content that may be necessary to support the auditing function includes time stamps, source and destination addresses, user or process identifiers, event descriptions, file names, and the access control or flow control rules that are invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred). Detailed information that organizations consider in audit records may include a full text recording of privileged commands or the individual identities of group account users.

分布式、基于事务的流程(例如，跨多个组织分布的流程)中的步骤，以及面向服务或基于云的架构中发生的操作。

监控和审计要求可以与其他系统需求相平衡。例如，组织可能确定系统必须具备记录每次文件访问(成功和不成功)的能力，但由于对系统性能的潜在负担，仅在特定情况下激活该能力。组织记录的事件类型可能随时间而变化。审查和更新已记录事件类型的集合是必要的，以确保当前的事件类型集合保持相关性。

参考文献

源控制：AU-02

支持性出版物：SP 800-92[35]

03.03.02 审计记录内容

a. 在审计记录中包含以下内容：
   1. 发生了什么类型的事件
   2. 当事件发生时
   3. 事件发生地点
   4. 事件来源
   5. 事件结果
   6. 与事件相关的个人、主体、对象或实体的身份

b. 根据需要为审计记录提供附加信息。

讨论

支持审计功能可能需要的审计记录内容包括时间戳、源地址和目的地址、用户或进程标识符、事件描述、文件名以及所调用的访问控制或流控制规则。事件结果可以包括事件成功或失败的指标以及事件特定的结果(例如，事件发生后系统的安全状态)。组织在审计记录中考虑的详细信息可以包括特权命令的全文记录或组账户用户的个人身份。

REFERENCES

Source Controls: AU-03, AU-03(01)

Supporting Publications: None

03.03.03 Audit Record Generation

a. Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02.

b. Retain audit records for a time period consistent with the records retention policy.

DISCUSSION

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records, including the access control or flow control rules invoked and the individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements.

REFERENCES

Source Controls: AU-11, AU-12

Supporting Publications: SP 800-92 [35]

03.03.04 Response to Audit Logging Process Failures

a. Alert organizational personnel or roles within [*Assignment: organization-defined time period*] in the event of an audit logging process failure.

b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

DISCUSSION

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Response actions include overwriting the oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of

参考文献

源控制：AU-03、AU-03(01)

支持性出版物：无

03.03.03 审计记录生成

a. 为03.03.01和03.03.02中指定的选定事件类型和审计记录内容生成审计记录。

b. 按照记录保留策略保留审计记录一段时间。

讨论

审计记录可以在不同的抽象层次上生成，包括在信息穿越网络时的数据包级别。选择适当的抽象层次是审计日志能力的关键方面，有助于识别问题的根本原因。添加审计记录中生成信息的能力取决于系统配置审计记录内容的功能。组织可以考虑在审计记录中添加额外信息，包括所调用的访问控制或流控制规则以及组账户用户的个人身份。组织还可以考虑将额外的审计记录信息限制为审计要求明确所需的信息。

参考文献

源控制：AU-11、AU-12

支持性出版物：SP 800-92[35]

03.03.04 对审计日志记录过程故障的响应

a. 在审计日志记录过程发生故障时，在[分配：组织定义的时间段]内向组织人员或角色发出警报。

b. 采取以下附加措施：[分配：组织定义的附加措施]。

讨论

审计日志记录过程故障包括软件和硬件错误、审计日志捕获机制故障以及达到或超过审计日志存储容量。响应措施包括覆盖最旧的审计记录、关闭系统以及停止生成审计记录。组织可以根据故障类型、故障位置、故障严重程度或这些因素的组合，选择为审计日志记录过程故障定义附加措施。

such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

REFERENCES

Source Control: AU-05

Supporting Publications: None

03.03.05 Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications and the potential impact of inappropriate or unusual activity.

b. Report findings to organizational personnel or roles.

c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

DISCUSSION

Audit record review, analysis, and reporting cover information security logging performed by organizations and can include logging that results from the monitoring of account usage, remote access, wireless connectivity, configuration settings, the use of maintenance tools and nonlocal maintenance, system component inventory, mobile device connection, equipment delivery and removal, physical access, temperature and humidity, communications at system interfaces, and the use of mobile code. Findings can be reported to organizational entities, such as the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The scope, frequency, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received. Correlating audit record review, analysis, and reporting processes helps to ensure that audit records collectively create a more complete view of events.

REFERENCES

Source Controls: AU-06, AU-06(03)

Supporting Publications: SP 800-86 [36], SP 800-101 [37]

当审计日志记录过程故障与存储相关时，针对审计日志存储库(即存储审计日志的独立系统组件)、审计日志所在的系统、组织的审计日志总存储容量(即所有审计日志存储库的总和)或三者全部执行响应。组织可以决定在向指定角色或人员发出警报后不采取附加措施。

参考文献

源控制：AU-05

支持性出版物：无

03.03.05 审计记录审查、分析与报告

a. [分配：组织定义的频率]审查和分析系统审计记录，以发现不当或异常活动的迹象及其潜在影响。

b. 向组织人员或角色报告发现。

c. 分析并关联不同存储库中的审计记录，以获得组织范围的态势感知。

讨论

审计记录审查、分析和报告涵盖组织执行的信息安全日志记录，可以包括因监控账户使用、远程访问、无线连接、配置设置、维护工具和非本地维护的使用、系统组件清单、移动设备连接、设备交付和移除、物理访问、温度和湿度、系统接口通信以及移动代码使用而产生的日志记录。发现的问题可以报告给组织实体，如事件响应团队、帮助台以及安全或隐私办公室。如果组织被禁止审查和分析审计记录或无法开展此类活动，审查或分析可以由获得此类授权的其他组织执行。审计记录审查、分析和报告的范围、频率和/或深度可以根据收到的新信息进行调整以满足组织需求。关联审计记录审查、分析和报告流程有助于确保审计记录共同创建更完整的事件视图。

参考文献

源控制：AU-06、AU-06(03)

支持性出版物：SP 800-86[36]、SP 800-101[37]

03.03.06 Audit Record Reduction and Report Generation

a. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents.

b. Preserve the original content and time ordering of audit records.

DISCUSSION

Audit records are generated in 03.03.03. Audit record reduction and report generation occur after audit record generation. Audit record reduction is a process that manipulates collected audit information and organizes it in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always come from the same system or organizational entities that conduct auditing activities. An audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. The time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

REFERENCES

Source Control: AU-07

Supporting Publications: None

03.03.07 Time Stamps

a. Use internal system clocks to generate time stamps for audit records.

b. Record time stamps for audit records that meet [*Assignment: organization-defined granularity of time measurement*] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.

DISCUSSION

Time stamps generated by the system include the date and time. Time is often expressed in Coordinated Universal Time (UTC) — a modern continuation of Greenwich Mean Time (GMT) — or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds or tens of milliseconds). Organizations may define different time granularities for system components. Time service can be critical to other security capabilities (e.g., access control and identification and authentication), depending on the nature of the mechanisms used to support those capabilities.

03.03.06 审计记录缩减与报告生成

a. 实施审计记录缩减和报告生成能力，以支持审计记录审查、分析、报告要求以及事件的事后调查。

b. 保留审计记录的原始内容和时间顺序。

讨论

审计记录在03.03.03中生成。审计记录缩减和报告生成在审计记录生成之后进行。审计记录缩减是一个处理收集的审计信息并将其组织为对分析人员更有意义的摘要格式的过程。审计记录缩减和报告生成能力并不总是来自执行审计活动的同一系统或组织实体。审计记录缩减能力可以包括例如具有高级数据过滤器的现代数据挖掘技术，以识别审计记录中的异常行为。系统提供的报告生成能力可以帮助生成可自定义的报告。如果记录中时间戳的粒度不足，审计记录的时间排序可能是一个重要问题。

参考文献

源控制：AU-07

支持性出版物：无

03.03.07 时间戳

a. 使用内部系统时钟为审计记录生成时间戳。

b. 为审计记录记录满足[分配：组织定义的时间测量粒度]的时间戳，并使用协调世界时(UTC)、具有相对于UTC的固定本地时间偏移，或将本地时间偏移作为时间戳的一部分。

讨论

系统生成的时间戳包括日期和时间。时间通常表示为协调世界时(UTC)--格林威治标准时间(GMT)的现代延续--或带有UTC偏移的本地时间。时间测量的粒度是指系统时钟与参考时钟之间的同步程度(例如，在数百或数十毫秒内同步的时钟)。组织可以为系统组件定义不同的时间粒度。时间服务对其他安全能力(例如，访问控制以及标识和身份验证)可能至关重要，这取决于用于支持这些能力的机制的性质。

REFERENCES

Source Control: AU-08

Supporting Publications: None

03.03.08 Protection of Audit Information

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

b. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.

DISCUSSION

Audit information includes the information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are programs and devices used to conduct audit and logging activities. The protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. The physical protection of audit information is addressed by media and physical protection requirements.

Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

REFERENCES

Source Controls: AU-09, AU-09(04)

Supporting Publications: None

03.03.09 Withdrawn

Incorporated into 03.03.08.

3.4. Configuration Management

03.04.01 Baseline Configuration

a. Develop and maintain under configuration control, a current baseline configuration of the system.

参考文献

源控制：AU-08

支持性出版物：无

03.03.08 审计信息的保护

a. 保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。

b. 仅授权部分特权用户或角色访问审计日志记录功能的管理。

讨论

审计信息包括成功审计系统活动所需的信息，例如审计记录、审计日志设置、审计报告和个人可识别信息。审计日志工具是用于开展审计和日志记录活动的程序和设备。审计信息的保护侧重于技术保护，并将访问和执行审计日志工具的能力限制为授权个人。审计信息的物理保护由介质和物理保护要求来解决。

对系统具有特权访问权限且同时是该系统审计对象的个人或角色，可能通过抑制审计活动或修改审计记录来影响审计信息的可靠性。要求进一步在审计相关特权和其他特权之间界定特权访问，可限制具有审计相关特权的用户或角色数量。

参考文献

源控制：AU-09、AU-09(04)

支持性出版物：无

03.03.09 已撤回

已纳入03.03.08。

3.4. 配置管理

03.04.01 基线配置

a. 在配置控制下开发和维护系统的当前基线配置。

b. Review and update the baseline configuration of the system [*Assignment: organization-defined frequency*] and when system components are installed or modified.

DISCUSSION

Baseline configurations for the system and system components include aspects of connectivity, operation, and communications. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for the system or configuration items within the system. Baseline configurations serve as a basis for future builds, releases, or changes to the system and include information about system components, operational procedures, network topology, and the placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as the system changes over time. Baseline configurations of the system reflect the current enterprise architecture.

REFERENCES

Source Control: CM-02

Supporting Publications: SP 800-124 [28], SP 800-128 [41], IR 8011-2 [42], IR 8011-3 [43]

03.04.02 Configuration Settings

a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [*Assignment: organization-defined configuration settings*].

b. Identify, document, and approve any deviations from established configuration settings.

DISCUSSION

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system and that affect the security posture or functionality of the system. Security-related configuration settings can be defined for systems (e.g., servers, workstations), input and output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Security parameters are those parameters that impact the security state of the system, including the parameters required to satisfy other security requirements. Security parameters include registry settings; account, file, and directory permission settings (i.e., privileges); and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and

b. [分配：组织定义的频率]以及在系统组件安装或修改时，审查和更新系统的基线配置。

讨论

系统和系统组件的基线配置包括连接性、运行和通信等方面。基线配置是经过记录、正式评审并达成一致的系统或系统内配置项的规范。基线配置作为系统未来构建、发布或变更的基础，并包含有关系统组件、操作程序、网络拓扑以及组件在系统架构中放置位置的信息。维护基线配置需要随着系统随时间变化而创建新的基线。系统的基线配置反映当前的企业架构。

参考文献

源控制：CM-02

支持性出版物：SP 800-124[28]、SP 800-128[41]、IR 8011-2[42]、IR 8011-3 [43]

03.04.02 配置设置

a. 为系统建立、记录并实施以下反映与运行要求一致的最严格模式的配置设置：[分配：组织定义的配置设置]。

b. 识别、记录并批准对既定配置设置的任何偏离。

讨论

配置设置是系统硬件、软件或固件组件中可更改的一组参数，这些参数影响系统的安全态势或功能。可以为系统(例如服务器、工作站)、输入和输出设备(例如扫描仪、复印机、打印机)、网络组件(例如防火墙、路由器、网关、语音和数据交换机、无线接入点、网络设备、传感器)、操作系统、中间件和应用程序定义与安全相关的配置设置。

安全参数是那些影响系统安全状态的参数，包括满足其他安全要求所需的参数。安全参数包括注册表设置；账户、文件和目录权限设置(即特权)；以及功能、端口、协议和远程连接的设置。组织建立组织范围的配置设置，并

subsequently derive specific configuration settings for the system. The established settings become part of the system's configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

REFERENCES

Source Control: CM-06

Supporting Publications: SP 800-70 [44], SP 800-126 [45], SP 800-128 [41]

03.04.03 Configuration Change Control

a. Define the types of changes to the system that are configuration-controlled.

b. Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.

c. Implement and document approved configuration-controlled changes to the system.

d. Monitor and review activities associated with configuration-controlled changes to the system.

DISCUSSION

Configuration change control refers to tracking, reviewing, approving or disapproving, and logging changes to the system. Specifically, it involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the system, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for system components (e.g., operating systems, applications, firewalls, routers, mobile devices) and configuration items of the system, changes to configuration settings, unscheduled and unauthorized changes, and changes to remediate vulnerabilities. This requirement is related to 03.04.04.

REFERENCES

Source Control: CM-03

Supporting Publications: SP 800-124 [28], SP 800-128 [41]

随后推导出系统的特定配置设置。已建立的设置成为系统配置基线的一部分。

通用安全配置(也称为安全配置检查表、锁定和加固指南、安全参考指南和安全技术实施指南)提供公认的、标准化的和既定的基准，这些基准规定了特定信息技术平台/产品的安全配置设置，以及将这些系统组件配置为满足操作要求的说明。通用安全配置可由各种组织制定，包括信息技术产品开发商、制造商、供应商、联盟、学术界、行业、联邦机构以及公共和私营部门的其他组织。

参考文献

源控制：CM-06

支持性出版物：SP 800-70[44]、SP 800-126[45]、SP 800-128[41]

03.04.03 配置变更控制

a. 定义受配置控制的系统变更类型。

b. 审查提议的受配置控制的系统变更，并在明确考虑安全影响的情况下批准或不批准此类变更。

c. 实施并记录经批准的、受配置控制的系统变更。

d. 监控和审查与受配置控制的系统变更相关的活动。

讨论

配置变更控制是指跟踪、评审、批准或不批准以及记录系统变更。具体而言，它涉及系统变更(包括系统升级和修改)的系统化提议、论证、实施、测试、评审和处置。配置变更控制包括对系统组件(例如操作系统、应用程序、防火墙、路由器、移动设备)的基线配置和系统配置项的变更、配置设置的变更、计划外和未经授权的变更，以及修复漏洞的变更。本要求与 03.04.04 相关。

参考文献

源控制：CM-03

支持性出版物：SP 800-124[28]、SP 800-128[41]

03.04.04 Impact Analyses

a. Analyze changes to the system to determine potential security impacts prior to change implementation.

b. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.

DISCUSSION

Organizational personnel with security responsibilities conduct impact analyses that include reviewing system security plans, policies, and procedures to understand security requirements; reviewing system design documentation and operational procedures to understand how system changes might affect the security state of the system; reviewing the impacts of system changes on supply chain partners with stakeholders; and determining how potential changes to a system create new risks and the ability to mitigate those risks. Impact analyses also include risk assessments to understand the impacts of changes and determine whether additional security requirements are needed. Changes to the system may affect the safeguards and countermeasures previously implemented. This requirement is related to 03.04.03. Not all changes to the system are configuration controlled.

REFERENCES

Source Controls: CM-04, CM-04(02)

Supporting Publications: SP 800-128 [41]

03.04.05 Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

DISCUSSION

Changes to the hardware, software, or firmware components of the system or the operational procedures related to the system can have potentially significant effects on the security of the system. Therefore, organizations permit only qualified and authorized individuals to access the system for the purpose of initiating changes. Access restrictions include physical and logical access controls, software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into the system), and change windows (i.e., changes occur only during specified times).

REFERENCES

Source Control: CM-05

Supporting Publications: FIPS 140-3 [38], FIPS 180-4 [39], SP 800-128 [41]

03.04.04 影响分析

a. 在实施变更之前分析系统变更以确定潜在的安全影响。

b. 验证在系统变更实施后，系统的安全要求是否继续得到满足。

讨论

负有安全责任的组织人员开展影响分析，包括评审系统安全计划、策略和程序以理解安全要求；评审系统设计文档和操作程序以理解系统变更可能如何影响系统的安全状态；与利益相关方一起评审系统变更对供应链合作伙伴的影响；以及确定系统的潜在变更如何产生新风险以及缓解这些风险的能力。影响分析还包括风险评估，以理解变更的影响并确定是否需要额外的安全要求。系统的变更可能影响先前实施的保障措施和对策。本要求与03.04.03相关。并非所有系统变更都受配置控制。

参考文献

源控制：CM-04、CM-04(02)

支持性出版物：SP 800-128[41]

03.04.05 变更访问限制

定义、记录、批准并执行与系统变更相关的物理和逻辑访问限制。

讨论

对系统硬件、软件或固件组件或与系统相关的操作程序的更改可能对系统的安全性产生潜在的重大影响。因此，组织仅允许合格且经授权的人员访问系统以发起更改。访问限制包括物理和逻辑访问控制、软件库、工作流自动化、媒体库、抽象层(即，更改实施到外部接口而非直接实施到系统中)以及更改窗口(即，更改仅在指定时间内发生)。

参考文献

源控制：CM-05

支持性出版物：FIPS 140-3[38]、FIPS 180-4[39]、SP 800-128[41]

03.04.06 Least Functionality

a. Configure the system to provide only mission-essential capabilities.

b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [*Assignment: organization-defined functions, ports, protocols, connections, and services*].

c. Review the system [*Assignment: organization-defined frequency*] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

DISCUSSION

Systems can provide a variety of functions and services. Some functions and services that are routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. It may be convenient to provide multiple services from single system components. However, doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit functionality to a single function per component.

Organizations review the functions and services provided by the system or system components to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent the unauthorized connection of devices, the transfer of information, and tunneling. Organizations can employ network scanning tools, intrusion detection and prevention systems, and endpoint protection systems (e.g., firewalls and host-based intrusion detection systems) to identify and prevent the use of prohibited functions, ports, protocols, system connections, and services. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of the types of protocols that organizations consider eliminating, restricting, or disabling.

REFERENCES

Source Controls: CM-07, CM-07(01)

Supporting Publications: SP 800-160-1 [11], SP 800-167 [46]

03.04.07 Withdrawn

Incorporated into 03.04.06 and 03.04.08.

03.04.08 Authorized Software – Allow by Exception

a. Identify software programs authorized to execute on the system.

03.04.06 最小功能

a. 将系统配置为仅提供任务必需的能力。

b. 禁止或限制使用以下功能、端口、协议、连接和服务：[分配：组织定义的功能、端口、协议、连接和服务]。

c. [分配：组织定义的频率]审查系统，以识别不必要或不安全的功能、端口、协议、连接和服务。

d. 禁用或移除不必要或不安全的功能、端口、协议、连接和服务。

讨论

系统可以提供各种功能和服务。某些默认例行提供的功能和服务可能并非支持基本组织任务、功能或运行所必需。从单个系统组件提供多个服务可能很方便。然而，这样做比限制任何单个组件提供的服务会增加风险。在可行的情况下，组织将功能限制为每个组件单一功能。

组织审查系统或系统组件所提供的功能和服务，以确定哪些功能和服务是可供消除的候选对象。组织禁用未使用或不必要的物理和逻辑端口及协议，以防止设备的未经授权连接、信息传输和隧道传输。组织可采用网络扫描工具、入侵检测和防御系统以及端点保护系统(例如，防火墙和基于主机的入侵检测系统)来识别并防止使用被禁止的功能、端口、协议、系统连接和服务。蓝牙、文件传输协议(FTP)和对等网络是组织考虑消除、限制或禁用的协议类型示例。

参考文献

源控制：CM-07、CM-07(01)

支持性出版物：SP 800-160-1[11]、SP 800-167[46]

03.04.07 已撤回

已纳入03.04.06和03.04.08。

03.04.08 授权软件 - 例外允许

a. 识别授权在系统上执行的软件程序。

b. Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.

c. Review and update the list of authorized software programs [*Assignment: organization-defined frequency*].

DISCUSSION

If provided with the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved "app stores." The policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Authorized software programs can be limited to specific versions or come from specific sources. To facilitate a comprehensive authorized software process and increase the strength of protection against attacks that bypass application-level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries.

REFERENCES

Source Control: CM-07(05)

Supporting Publications: SP 800-160-1 [11], SP 800-167 [46]

03.04.09 Withdrawn

Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.

03.04.10 System Component Inventory

a. Develop and document an inventory of system components.

b. Review and update the system component inventory [*Assignment: organization-defined frequency*].

c. Update the system component inventory as part of installations, removals, and system updates.

DISCUSSION

System components are discrete, identifiable assets (i.e., hardware, software, and firmware elements) that compose a system. Organizations may implement

b. 对系统上授权软件程序的执行实施拒绝所有、按例外允许的策略。

c. 审查并更新授权软件程序清单[赋值：组织定义的频率]。

讨论

如果被授予必要的权限，用户可以在组织系统中安装软件。为了保持对已安装软件的控制，组织确定有关软件安装的允许和禁止操作。允许的软件安装包括对现有软件的更新和安全补丁，以及从组织批准的"应用商店"下载新应用程序。为管理用户安装的软件而选择的策略由组织制定或由某些外部实体提供。策略执行方法可包括程序方法和自动化方法。

经授权的软件程序可以限于特定版本或来自特定来源。为了促进全面的经授权软件流程并增强对绕过应用级经授权软件的攻击的防护强度，软件程序可被分解并在不同详细级别上进行监控。这些级别包括应用程序、应用程序编程接口、应用程序模块、脚本、系统进程、系统服务、内核功能、注册表、驱动程序和动态链接库。

参考文献

源控制：CM-07(05)

支持性出版物：SP 800-160-1[11]、SP 800-167[46]

03.04.09 已撤回

由03.01.05、03.01.06、03.01.07、03.04.08和03.12.03处理。

03.04.10 系统组件清单

a. 制定并记录系统组件清单。

b. 审查并更新系统组件清单[赋值：组织定义的频率]。

c. 在安装、移除和系统更新过程中更新系统组件清单。

讨论

系统组件是构成系统的离散、可识别的资产(即硬件、软件和固件元素)。组织可以实施

centralized system component inventories that include components from all systems. In such situations, organizations ensure that the inventories include the system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, software license information, hardware inventory specifications, and — for networked components — the machine names and network addresses for all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include component type, physical location, date of receipt, manufacturer, cost, model, serial number, and supplier information.

REFERENCES

Source Controls: CM-08, CM-08(01)

Supporting Publications: SP 800-124 [28], SP 800-128 [41], IR 8011-2 [42], IR 8011-3 [43]

03.04.11 Information Location

a. Identify and document the location of CUI and the system components on which the information is processed and stored.

b. Document changes to the system or system component location where CUI is processed and stored.

DISCUSSION

Information location addresses the need to understand the specific system components where CUI is being processed and stored and the users who have access to CUI so that appropriate protection mechanisms can be provided, including information flow controls, access controls, and information management.

REFERENCES

Source Control: CM-12

Supporting Publications: None

03.04.12 System and Component Configuration for High-Risk Areas

a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [*Assignment: organization-defined system configurations*].

b. Apply the following security requirements to the systems or components when the individuals return from travel: [*Assignment: organization-defined security requirements*].

包含来自所有系统的组件的集中式系统组件清单。在此类情况下，组织确保清单包含组件问责所需的系统特定信息。系统组件有效问责所需的信息包括系统名称、软件所有者、软件版本号、软件许可证信息、硬件清单规格，以及--对于联网组件--所有已实施协议(例如，IPv4、IPv6)的机器名称和网络地址。清单规格包括组件类型、物理位置、接收日期、制造商、成本、型号、序列号和供应商信息。

参考文献

源控制：CM-08、CM-08(01)

支持性出版物：SP 800-124[28]、SP 800-128[41]、IR 8011-2[42]、IR 8011-3[43]

03.04.11 信息位置

a. 识别并记录 CUI 的位置以及处理和存储该信息的系统组件。

b. 记录处理和存储 CUI 的系统或系统组件位置的变化。

讨论

信息位置涉及理解处理和存储 CUI 的具体系统组件以及有权访问 CUI 的用户的需求，以便提供适当的保护机制，包括信息流控制、访问控制和信息管理。

参考文献

源控制：CM-12

支持性出版物：无

03.04.12 高风险区域的系统与组件配置

a. 向前往高风险地点的个人发放具有以下配置的系统或系统组件：[赋值：组织定义的系统配置]。

b. 当个人旅行返回时，对系统或组件应用以下安全要求：[赋值：组织定义的安全要求]。

DISCUSSION

When it is known that a system or a system component will be in a high-risk area, additional security requirements may be needed to counter the increased threat. Organizations can implement protective measures on the systems or system components used by individuals departing on and returning from travel. Actions include determining whether the locations are of concern, defining the required configurations for the components, ensuring that the components are configured as intended before travel is initiated, and taking additional actions after travel is completed. For example, systems going into high-risk areas can be configured with sanitized hard drives, limited applications, and more stringent configuration settings. Actions applied to mobile devices upon return from travel include examining the device for signs of physical tampering and purging and reimaging the device storage.

REFERENCES

Source Control: CM-02(07)

Supporting Publications: SP 800-124 [28], SP 800-128 [41]

3.5. Identification and Authentication

03.05.01 User Identification and Authentication

a. Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.

b. Re-authenticate users when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

DISCUSSION

System users include individuals (or system processes acting on behalf of individuals) who are authorized to access a system. Typically, individual identifiers are the usernames associated with the system accounts assigned to those individuals. Since system processes execute on behalf of groups and roles, organizations may require the unique identification of individuals in group accounts or the accountability of individual activity. The unique identification and authentication of users apply to all system accesses. Organizations use passwords, physical authenticators, biometrics, or some combination thereof to authenticate user identities. Organizations may re-authenticate individuals in certain situations, including when roles, authenticators, or credentials change; when the execution of privileged functions occurs; after a fixed time period; or periodically.

讨论

当已知系统或系统组件将处于高风险区域时，可能需要额外的安全要求来应对增加的威胁。组织可以对出行和返回人员所使用的系统或系统组件实施保护措施。措施包括确定相关地点是否值得关注、定义组件所需的配置、确保在出行开始前组件已按预期配置，以及在出行完成后采取额外措施。例如，进入高风险区域的系统可以配置为使用经过清理的硬盘、受限的应用程序以及更严格的配置设置。出行返回后对移动设备采取的措施包括检查设备是否有物理篡改迹象，以及清除并重新镜像设备存储。

参考文献

源控制：CM-02(07)

支持性出版物：SP 800-124[28]、SP 800-128[41]

3.5. 身份识别与身份验证

03.05.01 用户标识与身份验证

a. 唯一识别并身份验证系统用户，并将该唯一标识与代表这些用户行事的进程相关联。

b. 在[赋值：需要重新身份验证的组织定义情形或情况]时重新身份验证用户。

讨论

系统用户包括被授权访问系统的个人(或代表个人行事的系统进程)。通常，个人标识符是与分配给这些个人的系统账户相关联的用户名。由于系统进程代表组和角色执行，组织可能要求对组账户中的个人进行唯一标识或对个人活动进行问责。用户的唯一标识和身份验证适用于所有系统访问。组织使用密码、物理验证器、生物识别或其某种组合来验证用户身份。组织可能在特定情况下重新验证个人身份，包括角色、验证器或凭证发生变化时；执行特权功能时；固定时间段之后；或定期进行。

REFERENCES

Source Controls: IA-02, IA-11

Supporting Publications: SP 800-63-3 [27]

03.05.02 Device Identification and Authentication

Uniquely identify and authenticate [*Assignment: organization-defined devices or types of devices*] before establishing a system connection.

DISCUSSION

Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Public Key Infrastructure (PKI) and certificate revocation checking for the certificates exchanged can be included as part of device authentication.

REFERENCES

Source Control: IA-03

Supporting Publications: SP 800-63-3 [27]

03.05.03 Multi-Factor Authentication

Implement multi-factor authentication for access to privileged and non-privileged accounts.

DISCUSSION

This requirement applies to user accounts. Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator, such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level to provide increased information security.

参考文献

源控制：IA-02、IA-11

支持性出版物：SP 800-63-3[27]

03.05.02 设备标识与认证

在建立系统连接之前唯一识别并身份验证[赋值：组织定义的设备或设备类型]。

讨论

需要唯一设备到设备标识和身份验证的设备由类型、设备或类型与设备的组合来定义。组织定义的设备类型包括不属于组织所有的设备。系统使用共享的已知信息(例如，媒体访问控制[MAC]、传输控制协议/互联网协议[TCP/IP]地址)进行设备标识，或使用组织身份验证解决方案(例如，电气和电子工程师协会[IEEE] 802.1x和可扩展身份验证协议[EAP]、使用EAP-传输层安全[TLS]身份验证的RADIUS服务器、Kerberos)来标识和验证局域网和广域网上的设备。公钥基础设施(PKI)和对所交换证书的证书吊销检查可以作为设备身份验证的一部分。

参考文献

源控制：IA-03

支持性出版物：SP 800-63-3[27]

03.05.03 多因素认证

对特权账户和非特权账户的访问实施多因素身份验证。

讨论

本要求适用于用户账户。多因素身份验证要求使用两个或多个不同的因素来实现身份验证。身份验证因素定义如下：你知道的某物(例如，个人识别码[PIN])、你拥有的某物(例如，物理验证器，如加密私钥)或你本身的特征(例如，生物识别)。具有物理验证器的多因素身份验证解决方案包括提供基于时间或挑战-响应输出的硬件验证器和智能卡。除了在系统级别对用户进行身份验证外，组织还可以在应用程序级别采用身份验证机制，以提供更高的信息安全。

REFERENCES

Source Controls: IA-02(01), IA-02(02)

Supporting Publications: SP 800-63-3 [27]

03.05.04 Replay-Resistant Authentication

Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

DISCUSSION

Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges, such as time synchronous or challenge-response one-time authenticators.

REFERENCES

Source Control: IA-02(08)

Supporting Publications: SP 800-63-3 [27]

03.05.05 Identifier Management

a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

b. Select and assign an identifier that identifies an individual, group, role, service, or device.

c. Prevent the reuse of identifiers for [*Assignment: organization-defined time period*].

d. Manage individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].

DISCUSSION

Identifiers are provided for users, processes acting on behalf of users, and devices. Prohibiting the reuse of identifiers prevents the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides information about the people with whom organizational personnel are communicating. For example, it is useful for an employee to know that one of the individuals on an email message is a contractor.

参考文献

源控制：IA-02(01), IA-02(02)

支持性出版物：SP 800-63-3[27]

03.05.04 抗重放认证

对特权账户和非特权账户的访问实施抗重放身份验证机制。

讨论

如果通过记录或重放先前的身份验证消息来成功进行身份验证是不切实际的，则身份验证过程可抵抗重放攻击。抗重放技术包括使用随机数或挑战的协议，例如时间同步或挑战-响应一次性身份验证器。

参考文献

源控制：IA-02(08)

支持性出版物：SP 800-63-3[27]

03.05.05 标识符管理

a. 获得组织人员或角色的授权，以分配个人、组、角色、服务或设备标识符。

b. 选择并分配标识个人、组、角色、服务或设备的标识符。

c. 防止在[赋值：组织定义的时间段]内重用标识符。

d. 通过将每个个人唯一标识为[赋值：标识个人状态的组织定义特征]来管理个人标识符。

讨论

为用户、代表用户行事的进程和设备提供标识符。禁止重用标识符可防止将先前使用的个人、组、角色、服务或设备标识符分配给不同的个人、组、角色、服务或设备。

标识个人状态的特征包括承包商、外国国民和非组织用户。通过这些特征标识个人状态可提供有关组织人员正在与之通信的人员的信息。例如，员工知道电子邮件消息中的某个人是承包商是有用的。

REFERENCES

Source Controls: IA-04, IA-04(04)

Supporting Publications: SP 800-63-3 [27]

03.05.06 Withdrawn

Consistency with SP 800-53 [8].

03.05.07 Password Management

a. Maintain a list of commonly-used, expected, or compromised passwords, and update the list [*Assignment: organization-defined frequency*] and when organizational passwords are suspected to have been compromised.

b. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.

c. Transmit passwords only over cryptographically protected channels.

d. Store passwords in a cryptographically protected form.

e. Select a new password upon first use after account recovery.

f. Enforce the following composition and complexity rules for passwords: [*Assignment: organization-defined composition and complexity rules*].

DISCUSSION

Password-based authentication applies to passwords used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable to shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish and enforce certain rules for password generation (e.g., minimum character length) under certain circumstances. For example, account recovery can occur when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof. Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity and reduces susceptibility to authenticator compromises. Long passwords and passphrases can be used to increase the complexity of passwords.

参考文献

源控制：IA-04、IA-04(04)

支持性出版物：SP 800-63-3[27]

03.05.06 已撤回

与 SP 800-53[8] 保持一致。

03.05.07 密码管理

a. 维护常用、预期或已泄露密码的清单，并[赋值：组织定义的频率]以及在怀疑组织密码已泄露时更新该清单。

b. 当用户创建或更新密码时，验证密码不在常用、预期或已泄露密码的清单上。

c. 仅通过加密保护的通道传输密码。

d. 以加密保护的形式存储密码。

e. 在账户恢复后首次使用时选择新密码。

f. 对密码强制执行以下组成和复杂性规则：[赋值：组织定义的组成和复杂性规则]。

讨论

基于密码的身份验证适用于单因素或多因素身份验证中使用的密码。长密码或口令短语优于较短的密码。强制组合规则提供的安全益处有限，同时会降低可用性。然而，组织可以选择在某些情况下建立并执行某些密码生成规则(例如，最小字符长度)。例如，当忘记密码时可以进行账户恢复。受加密保护的密码包括密码的加盐单向加密哈希。常用、已泄露或预期密码的列表包括从先前泄露语料库、字典单词以及重复或连续字符中获得的密码。该列表包括上下文特定的单词，例如服务名称、用户名及其衍生词。在系统登录后立即将临时密码更改为永久密码，可确保尽早实施身份验证机制的必要强度，并降低验证器被泄露的可能性。长密码和口令短语可用于增加密码的复杂性。

REFERENCES

Source Control: IA-05(01)

Supporting Publications: SP 800-63-3 [27]

03.05.08 Withdrawn

Consistency with SP 800-53 [8].

03.05.09 Withdrawn

Consistency with SP 800-53 [8].

03.05.10 Withdrawn

Incorporated into 03.05.07.

03.05.11 Authentication Feedback

Obscure feedback of authentication information during the authentication process.

DISCUSSION

Authentication feedback does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For example, for desktop or notebook systems with relatively large monitors, the threat may be significant (commonly referred to as shoulder surfing). For mobile devices with small displays, this threat may be less significant and is balanced against the increased likelihood of input errors due to small keyboards. Therefore, the means of obscuring authenticator feedback is selected accordingly. Obscuring feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a limited time before fully obscuring it.

REFERENCES

Source Control: IA-06

Supporting Publications: None

03.05.12 Authenticator Management

a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.

b. Establish initial authenticator content for any authenticators issued by the organization.

参考文献

源控制：IA-05(01)

支持性出版物：SP 800-63-3[27]

03.05.08 已撤回

与 SP 800-53[8] 保持一致。

03.05.09 已撤回

与 SP 800-53[8] 保持一致。

03.05.10 已撤回

已纳入03.05.07。

03.05.11 认证反馈

在身份验证过程中隐藏身份验证信息的反馈。

讨论

身份验证反馈不会提供可能使未经授权的个人破坏身份验证机制的信息。例如，对于显示器相对较大的台式机或笔记本电脑系统，该威胁可能很显著(通常称为肩窥)。对于显示屏较小的移动设备，该威胁可能不太显著，并且需要与因键盘较小而导致输入错误可能性增加这一情况相权衡。因此，会相应地选择遮蔽身份验证器反馈的方法。遮蔽反馈包括在用户向输入设备键入密码时显示星号，或在完全遮蔽反馈之前仅显示有限时间。

参考文献

源控制：IA-06

支持性出版物：无

03.05.12 认证器管理

a. 作为初始身份验证器分发的一部分，验证接收身份验证器的个人、组、角色、服务或设备的身份。

b. 为组织发放的任何身份验证器建立初始身份验证器内容。

c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.

d. Change default authenticators at first use.

e. Change or refresh authenticators [*Assignment: organization-defined frequency*] or when the following events occur: [*Assignment: organization-defined events*].

f. Protect authenticator content from unauthorized disclosure and modification.

DISCUSSION

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. The initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, requirements for authenticator content contain specific characteristics. Authenticator management is supported by organization-defined settings and restrictions for various authenticator characteristics (e.g., password complexity and composition rules, validation time window for time synchronous one-time tokens, and the number of allowed rejections during the verification stage of biometric authentication).

The requirement to protect individual authenticators may be implemented by 03.15.03 for authenticators in the possession of individuals and by 03.01.01, 03.01.02, 03.01.05, and 03.13.08 for authenticators stored in organizational systems. This includes passwords stored in hashed or encrypted formats or files that contain hashed or encrypted passwords that are accessible with administrator privileges. Actions can be taken to protect authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators.

Developers may deliver system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well-known, easily discoverable, and present a significant risk. Authenticator management includes issuing and revoking authenticators for temporary access when they are no longer needed. The use of long passwords or passphrases may obviate the need to periodically change authenticators.

REFERENCES

Source Control: IA-05

Supporting Publications: SP 800-63-3 [27]

c. 建立并实施管理程序，用于初始身份验证器分发；丢失、泄露或损坏的身份验证器；以及撤销身份验证器。

d. 首次使用时更改默认认证器。

e. 在[赋值：组织定义的频率]或发生以下事件时更改或刷新身份验证器：[赋值：组织定义的事件]。

f. 保护认证器内容免遭未经授权的泄露和修改。

讨论

身份验证器包括密码、加密设备、生物识别、证书、一次性密码设备和 ID 徽章。初始身份验证器内容是身份验证器的实际内容(例如初始密码)。相比之下，身份验证器内容要求包含特定特征。身份验证器管理由组织定义的针对各种身份验证器特征的设置和限制提供支持(例如密码复杂度和组成规则、时间同步一次性令牌的验证时间窗口，以及生物识别身份验证验证阶段允许的拒绝次数)。

保护单个认证器的要求可通过以下方式实施：
03.15.03 对于个人持有的认证器，以及依据03.01.01，03.01.02、03.01.05和03.13.08适用于存储在组织系统中的身份验证器。这包括以哈希或加密格式存储的密码，或包含可通过管理员权限访问的哈希或加密密码的文件。可以采取行动保护身份验证器，包括保持对身份验证器的占有、不与他人共享身份验证器，以及立即报告丢失、被盗或泄露的身份验证器。

开发者可能交付带有出厂默认身份验证凭据的系统组件，以便进行初始安装和配置。默认身份验证凭据通常广为人知、易于发现，并构成重大风险。身份验证器管理包括在不再需要临时访问时发放和撤销身份验证器。使用长密码或口令短语可以免去定期更改身份验证器的需要。

参考文献

源控制：IA-05

支持性出版物：SP 800-63-3[27]

3.6. Incident Response

03.06.01 Incident Handling

Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

DISCUSSION

Incident-related information can be obtained from a variety of sources, including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. An effective incident handling capability involves coordination among many organizational entities, including mission and business owners, system owners, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.

REFERENCES

Source Controls: IR-04

Supporting Publications: SP 800-50 [32], SP 800-61 [47], SP 800-161 [33]

03.06.02 Incident Monitoring, Reporting, and Response Assistance

a. Track and document system security incidents.

b. Report suspected incidents to the organizational incident response capability within [*Assignment: organization-defined time period*].

c. Report incident information to [*Assignment: organization-defined authorities*].

d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.

DISCUSSION

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from many sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. 03.06.01 provides information on the types of incidents that are appropriate for monitoring. The types of incidents reported, the content and timeliness of the reports, and the reporting authorities reflect applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Incident information informs risk assessments, the

3.6. 事件响应

03.06.01 事件处理

实施与事件响应计划一致的事件处理能力，包括准备、检测与分析、遏制、根除和恢复。

讨论

事件相关信息可从多种来源获取，包括审计监控、网络监控、物理访问监控、用户和管理员报告以及报告的供应链事件。有效的事件处理能力涉及许多组织实体之间的协调，包括任务和业务所有者、系统所有者、人力资源办公室、物理和人员安全办公室、法律部门、运营人员和采购办公室。

参考文献

源控制：IR-04

支持性出版物：SP 800-50[32]、SP 800-61[47]、SP 800-161[33]

03.06.02 事件监控、报告与响应协助

a. 跟踪并记录系统安全事件。

b. 在[赋值：组织定义的时间段]内向组织事件响应能力报告可疑事件。

c. 向[赋值：组织定义的机构]报告事件信息。

d. 提供事件响应支持资源，就处理和报告事件向系统用户提供建议和协助。

讨论

记录事件包括维护关于每个事件的记录、事件状态以及取证所需的其他相关信息，以及评估事件详情、趋势和处理情况。事件信息可从许多来源获取，包括网络监控、事件报告、事件响应团队、用户投诉、供应链合作伙伴、审计监控、物理访问监控以及用户和管理员报告。03.06.01提供了适合监控的事件类型的信息。所报告的事件类型、报告的内容和及时性以及报告主管机构反映了适用的法律、行政命令、指令、法规、政策、标准和指南。事件信息为风险评估提供依据，

effectiveness of security assessments, the security requirements for acquisitions, and the selection criteria for technology products. Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensic services or consumer redress services, when required.

REFERENCES

Source Controls: IR-05, IR-06, IR-07

Supporting Publications: SP 800-61 [47], SP 800-86 [36]

03.06.03 Incident Response Testing

Test the effectiveness of the incident response capability [*Assignment: organization-defined frequency*].

DISCUSSION

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations. Incident response testing can include a determination of the effects of incident response on organizational operations, organizational assets, and individuals. Qualitative and quantitative data can help determine the effectiveness of incident response processes.

REFERENCES

Source Control: IR-03

Supporting Publications: SP 800-84 [48]

03.06.04 Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility or acquiring system access,
   2. When required by system changes, and
   3. [*Assignment: organization-defined frequency*] thereafter.

b. Review and update incident response training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

安全评估的有效性、采购的安全要求以及技术产品的选择标准。组织提供的事件响应支持资源包括帮助台、协助小组、用于开启和跟踪事件响应工单的自动化工单系统，以及在需要时获取取证服务或消费者补救服务。

参考文献

源控制：IR-05、IR-06、IR-07

支持性出版物：SP 800-61[47],SP 800-86[36]

03.06.03 事件响应测试

测试事件响应能力的有效性[赋值：组织定义的频率]。

讨论

组织测试事件响应能力以确定其有效性并识别潜在弱点或缺陷。事件响应测试包括使用检查表、走查或桌面演练以及模拟。事件响应测试可包括确定事件响应对组织运营、组织资产和个人的影响。定性和定量数据有助于确定事件响应流程的有效性。

参考文献

源控制：IR-03

支持性出版物：SP 800-84[48]

03.06.04 事件响应培训

a. 向系统用户提供与其分配的角色和职责一致的事件响应培训：
   1. 在承担事件响应角色或职责或获得系统访问权限后的[赋值：组织定义的时间段]内，
   2. 当系统变更要求时，并且
   3. [分配：组织定义的频率] 此后。

b. 按[赋值：组织定义的频率]并在此后[赋值：组织定义的事件]审查和更新事件响应培训内容。

DISCUSSION

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know how to recognize an incident or whom to call; system administrators may require additional training on how to handle incidents; and incident responders may receive specific training on data collection techniques, forensics, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of 03.02.02. Events that may cause an update to incident response training content include incident response plan testing, response to an actual incident, audit or assessment findings, or changes in applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

REFERENCES

Source Control: IR-02

Supporting Publications: SP 800-86 [36], SP 800-137 [49]

03.06.05 Incident Response Plan

a. Develop an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability,
   2. Describes the structure and organization of the incident response capability,
   3. Provides a high-level approach for how the incident response capability fits into the overall organization,
   4. Defines reportable incidents,
   5. Addresses the sharing of incident information, and
   6. Designates responsibilities to organizational entities, personnel, or roles.
b. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.
c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
d. Protect the incident response plan from unauthorized disclosure.

DISCUSSION

It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the

讨论

事件响应培训与组织人员被分配的角色和职责相关联，以确保此类培训包含适当的内容和详细程度。例如，用户可能只需要知道如何识别事件或联系谁；系统管理员可能需要关于如何处理事件的额外培训；事件响应人员可能接受关于数据收集技术、取证、报告、系统恢复和系统还原的特定培训。事件响应培训包括用户识别和报告来自外部和内部来源的可疑活动的培训。为用户提供的事件响应培训可作为03.02.02的一部分提供。可能导致更新事件响应培训内容的事件包括事件响应计划测试、对实际事件的响应、审计或评估发现，或适用法律、行政命令、政策、指令、法规、标准和指南的变化。

参考文献

源控制：IR-02

支持性出版物：SP 800-86[36]、SP 800-137[49]

03.06.05 事件响应计划

a. 制定一份事件响应计划，该计划应：
   1. 为组织提供实施其事件响应能力的路线图，
   2. 描述事件响应能力的结构与组织，
   3. 提供关于事件响应能力如何融入整个组织的高层方法，
   4. 定义可报告事件，
   5. 涉及事件信息的共享，以及
   6. 为组织实体、人员或角色指定职责。
b. 将事件响应计划的副本分发给指定的事件响应人员(按姓名和/或角色标识)和组织单元。
c. 更新事件响应计划，以应对系统和组织变更或在计划实施、执行或测试期间遇到的问题。
d. 保护事件响应计划免遭未经授权的披露。

讨论

组织制定和实施协调一致的事件响应方法非常重要。组织的任务和业务功能决定了

structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain.

REFERENCES

Source Control: IR-08

Supporting Publications: SP 800-86 [36], SP 800-137 [49]

3.7. Maintenance

03.07.01 Withdrawn

Recategorized as NCO.

03.07.02 Withdrawn

Incorporated into 03.07.04 and 03.07.06.

03.07.03 Withdrawn

Incorporated into 03.08.03.

03.07.04 Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools.

b. Check media with diagnostic and test programs for malicious code before it is used in the system.

c. Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.

DISCUSSION

Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with the tools that are used for diagnostic and repair actions on the system. Maintenance tools can include hardware and software diagnostic and test equipment as well as packet sniffers. The tools may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Diagnostic and test programs are potential vehicles for transporting malicious code into the system, either intentionally or unintentionally. Examples of media inspection include checking the cryptographic hash or digital signatures of diagnostic and test programs and media.

事件响应能力的结构。作为事件响应能力的一部分，组织考虑与外部组织(包括外部服务提供商和供应链中涉及的其他组织)协调和共享信息。

参考文献

源控制：IR-08

支持性出版物：SP 800-86[36]、SP 800-137[49]

3.7. 维护

03.07.01 已撤销

重新归类为NCO。

03.07.02 已撤回

已纳入03.07.04和03.07.06。

03.07.03 已撤销

已纳入03.08.03。

03.07.04 维护工具

a. 批准、控制和监控系统维护工具的使用。

b. 在系统使用介质之前，使用诊断和测试程序检查介质是否存在恶意代码。

c. 通过验证设备上不存在CUI、净化或销毁设备或将设备保留在设施内，防止包含CUI的系统维护设备被移出。

讨论

批准、控制、监控和审查维护工具解决与用于系统诊断和修复操作的工具相关的安全问题。维护工具可包括硬件和软件诊断和测试设备以及数据包嗅探器。这些工具可能是预安装的、由维护人员通过介质带入的、基于云的或从网站下载的。诊断和测试程序是潜在的将恶意代码有意或无意地传入系统的载体。介质检查的示例包括检查诊断和测试程序及介质的加密哈希或数字签名。

If organizations inspect media that contain diagnostic and test programs and determine that the media also contain malicious code, the incident is handled consistent with incident handling policies and procedures. A periodic review of system maintenance tools can result in the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools do not address the hardware and software components that support maintenance and are considered a part of the system.

REFERENCES

Source Controls: MA-03, MA-03(01), MA-03(02), MA-03(03)

Supporting Publications: SP 800-88 [50]

03.07.05 Nonlocal Maintenance

a. Approve and monitor nonlocal maintenance and diagnostic activities.

b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.

c. Terminate session and network connections when nonlocal maintenance is completed.

DISCUSSION

Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the location of the system and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the requirements in 03.05.01.

REFERENCES

Source Control: MA-04

Supporting Publications: SP 800-63-3 [27], SP 800-88 [50]

03.07.06 Maintenance Personnel

a. Establish a process for maintenance personnel authorization.

b. Maintain a list of authorized maintenance organizations or personnel.

c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.

如果组织检查包含诊断和测试程序的介质并确定该介质还包含恶意代码，则按照事件处理策略和程序处理该事件。对系统维护工具的定期审查可能导致撤销对过时、不受支持、无关或不再使用的工具的批准。维护工具不涉及支持维护且被视为系统一部分的硬件和软件组件。

参考文献

源控制：MA-03、MA-03(01)、MA-03(02)、MA-03(03)支持性出版物：SP 800-88[50]

03.07.05 非本地维护

a. 批准并监控非本地维护和诊断活动。

b. 在建立非本地维护和诊断会话时实施多因素身份验证和重放抵抗。

c. 非本地维护完成后终止会话和网络连接。

讨论

非本地维护和诊断活动由通过外部或内部网络通信的人员进行。本地维护和诊断活动由实际位于系统所在地且不通过网络连接通信的人员进行。用于建立非本地维护和诊断会话的身份验证技术反映03.05.01中的要求。

参考文献

源控制：MA-04

支持性出版物：SP 800-63-3[27]、SP 800-88[50]

03.07.06 维护人员

a. 为维护人员授权建立流程。

b. 维护授权维护组织或人员的清单。

c. 验证对系统执行维护的无陪同人员拥有所需的访问授权。

d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

DISCUSSION

Maintenance personnel refers to individuals who perform hardware or software maintenance on the system, while 03.10.01 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the system. The technical competence of supervising individuals relates to the maintenance performed on the system, while having required access authorizations refers to maintenance on and near the system. Individuals who have not been previously identified as authorized maintenance personnel (e.g., manufacturers, consultants, systems integrators, and vendors) may require privileged access to the system, such as when they are required to conduct maintenance with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on their risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

REFERENCES

Source Control: MA-05

Supporting Publications: None

3.8. Media Protection

03.08.01 Media Storage

Physically control and securely store system media that contain CUI.

DISCUSSION

System media include digital and non-digital media. Digital media include diskettes, flash drives, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media include paper and microfilm. Physically controlling stored media includes conducting inventories, establishing procedures to allow individuals to check out and return media to libraries, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. Controlled areas provide physical and procedural controls to meet the requirements established for protecting information and systems. Sanitization techniques (e.g., destroying, cryptographically erasing, clearing, and purging) prevent the disclosure of CUI to unauthorized individuals. The sanitization process removes CUI from media such that the information cannot be retrieved or reconstructed.

d. 指定具备所需访问授权和技术能力的组织人员，以监督不具备所需访问授权的人员的维护活动。

讨论

维护人员是指对系统执行硬件或软件维护的个人，而03.10.01涉及因维护职责而处于系统物理保护边界内的个人的物理访问。监督人员的技术能力与对系统执行的维护相关，而具备所需的访问授权则涉及对系统及系统附近的维护。先前未被识别为授权维护人员的个人(例如制造商、顾问、系统集成商和供应商)可能需要特权访问系统，例如当他们需要在几乎没有通知或没有通知的情况下进行维护时。组织可根据其风险评估选择向这些个人发放临时凭证。临时凭证可用于一次性使用或非常有限的时间段。

参考文献

源控制：MA-05

支持性出版物：无

3.8. 媒体保护

03.08.01 媒体存储

对包含CUI的系统介质进行物理控制和安全存储。

讨论

系统介质包括数字和非数字介质。数字介质包括软盘、闪存驱动器、磁带、外部或可移动固态或磁驱动器、光盘和数字多功能光盘。非数字介质包括纸张和缩微胶片。对存储介质进行物理控制包括进行清点、建立允许个人从库中借出和归还介质的程序，以及维护对存储介质的问责。安全存储包括上锁的抽屉、书桌或柜子，或受控的介质库。受控区域提供物理和程序控制，以满足为保护信息和系统而建立的要求。净化技术(例如销毁、加密擦除、清除和清理)防止CUI泄露给未经授权的个人。净化过程从介质中移除CUI，使得信息无法被检索或重建。

REFERENCES

Source Control: MP-04

Supporting Publications: SP 800-88 [50], SP 800-111 [51]

03.08.02 Media Access

Restrict access to CUI on system media to authorized personnel or roles.

DISCUSSION

System media include digital and non-digital media. Access to CUI on system media can be restricted by physically controlling such media. This includes conducting inventories, ensuring that procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for stored media. For digital media, access to CUI can be restricted by using cryptographic means. Encrypting data in storage or at rest is addressed in 03.13.08.

REFERENCES

Source Control: MP-02

Supporting Publications: SP 800-111 [51]

03.08.03 Media Sanitization

Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.

DISCUSSION

Media sanitization applies to digital and non-digital media that are subject to disposal or reuse, whether or not the media are considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, mobile devices, workstations, network components, and non-digital media. The sanitization process removes CUI from media such that the information cannot be retrieved or reconstructed. Sanitization techniques (e.g., cryptographically erasing, clearing, purging, and destroying) prevent the disclosure of CUI to unauthorized individuals when such media are reused or released for disposal. NARA policies control the sanitization process for media that contain CUI and may require destruction when other methods cannot be applied to the media.

REFERENCES

Source Control: MP-06

Supporting Publications: SP 800-88 [50]

参考文献

源控制：MP-04

支持性出版物：SP 800-88[50]、SP 800-111[51]

03.08.02 媒体访问

将系统介质上的 CUI 访问限制为授权人员或角色。

讨论

系统介质包括数字和非数字介质。系统介质上的CUI访问可以通过物理控制此类介质来限制。这包括进行清点、确保制定允许个人借出和归还介质到介质库的程序，以及维护对存储介质的问责。对于数字介质，可以通过使用加密手段限制对CUI的访问。存储中或静态数据的加密在03.13.08中处理。

参考文献

源控制：MP-02

支持性出版物：SP 800-111[51]

03.08.03 介质净化

在处置、释放出组织控制或释放以供重用之前，净化包含CUI的系统介质。

讨论

介质净化适用于需要处置或再利用的数字和非数字介质，无论这些介质是否被视为可移动介质。示例包括扫描仪、复印机、打印机、笔记本电脑、移动设备、工作站、网络组件中的数字介质以及非数字介质。净化过程从介质中移除CUI，使得信息无法被检索或重建。净化技术(例如加密擦除、清除、清理和销毁)防止在此类介质被再利用或释放处置时CUI泄露给未经授权的个人。NARA政策控制包含CUI的介质的净化过程，并且当其他方法无法应用于介质时可能要求销毁。

参考文献

源控制：MP-06

支持性出版物：SP 800-88[50]

03.08.04 Media Marking

Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.

DISCUSSION

System media include digital and non-digital media. Marking refers to the use or application of human-readable security attributes. Labeling refers to the use of security attributes for internal system data structures. Digital media include diskettes, magnetic tapes, external or removable solid state or magnetic drives, flash drives, compact discs, and digital versatile discs. Non-digital media include paper and microfilm. CUI is defined by NARA along with marking, safeguarding, and dissemination requirements for such information.

REFERENCES

Source Control: MP-03

Supporting Publications: None

03.08.05 Media Transport

a. Protect and control system media that contain CUI during transport outside of controlled areas.

b. Maintain accountability of system media that contain CUI during transport outside of controlled areas.

c. Document activities associated with the transport of system media that contain CUI.

DISCUSSION

System media include digital and non-digital media. Digital media include flash drives, diskettes, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media include microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural measures to meet the requirements established for protecting CUI and systems. Media protection during transport can include cryptography and/or locked containers. Activities associated with media transport include releasing media for transport, ensuring that media enter the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking or obtaining the records of transport activities as the media move through the transportation system to prevent and detect loss, destruction, or tampering. This requirement is related to 03.13.08 and 03.13.11.

03.08.04 介质标记

标记包含CUI的系统介质，以指示分发限制、处理注意事项和适用的CUI标记。

讨论

系统介质包括数字和非数字介质。标记是指使用或应用人类可读的安全属性。标签是指对内部系统数据结构使用安全属性。数字介质包括软盘、磁带、外部或可移动固态或磁驱动器、闪存驱动器、光盘和数字多功能光盘。非数字介质包括纸张和缩微胶片。CUI由NARA定义，并对此类信息的标记、保护和传播要求作出规定。

参考文献

源控制：MP-03

支持性出版物：无

03.08.05 介质传输

a. 在受控区域外运输期间保护和控制系统介质中的CUI。

b. 在受控区域外运输期间维护对包含CUI的系统介质的问责。

c. 记录与包含CUI的系统介质传输相关的活动。

讨论

系统介质包括数字和非数字介质。数字介质包括闪存驱动器、软盘、磁带、外部或可移动固态或磁驱动器、光盘和数字多功能光盘。非数字介质包括缩微胶片和纸张。受控区域是组织为其提供物理或程序措施以满足为保护CUI和系统而建立的要求的空间。运输期间的介质保护可包括密码学和/或上锁的容器。与介质运输相关的活动包括放行介质以供运输、确保介质进入适当的运输流程以及实际运输。授权运输和快递人员可包括组织外部人员。在运输期间维护介质的问责包括将运输活动限制于授权人员，并在介质通过运输系统移动时跟踪或获取运输活动的记录，以防止和检测丢失、销毁或篡改。本要求与03.13.08和03.13.11相关。

REFERENCES

Source Controls: MP-05, SC-28

Supporting Publications: SP 800-111 [51]

03.08.06 Withdrawn

Addressed by 03.13.08.

03.08.07 Media Use

a. Restrict or prohibit the use of [*Assignment: organization-defined types of system media*].

b. Prohibit the use of removable system media without an identifiable owner.

DISCUSSION

In contrast to requirement 03.08.01, which restricts user access to media, this requirement restricts or prohibits the use of certain types of media, such as external hard drives, flash drives, or smart displays. Organizations can use technical and non-technical measures (e.g., policies, procedures, and rules of behavior) to control the use of system media. For example, organizations may control the use of portable storage devices by using physical cages on workstations to prohibit access to external ports or disabling or removing the ability to insert, read, or write to devices.

Organizations may limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Organizations may also control the use of portable storage devices based on the type of device — prohibiting the use of writeable, portable devices — and implement this restriction by disabling or removing the capability to write to such devices. Limits on the use of organization-controlled system media in external systems include restrictions on how the media may be used and under what conditions. Requiring identifiable owners (e.g., individuals, organizations, or projects) for removable system media reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the media (e.g., insertion of malicious code).

REFERENCES

Source Control: MP-07

Supporting Publications: SP 800-111 [51]

参考文献

源控制：MP-05、SC-28

支持性出版物：SP 800-111[51]

03.08.06 已撤回

由03.13.08涵盖。

03.08.07 媒体使用

a. 限制或禁止使用[赋值：组织定义的系统介质类型]。

b. 禁止使用没有可识别所有者的可移动系统介质。

讨论

与限制用户访问媒体的要求03.08.01不同，本要求限制或禁止使用某些类型的媒体，例如外部硬盘驱动器、闪存驱动器或智能显示器。组织可以使用技术性和非技术性措施(例如政策、程序和行为规则)来控制系统媒体的使用。例如，组织可以通过在工作站上使用物理笼子来禁止访问外部端口，或禁用或移除插入、读取或写入设备的能力，从而控制便携式存储设备的使用。

组织可以将便携式存储设备的使用限制为仅限经批准的设备，包括组织提供的设备、其他经批准组织提供的设备以及非个人拥有的设备。组织还可以基于设备类型控制便携式存储设备的使用--禁止使用可写的便携式设备--并通过禁用或移除写入此类设备的能力来实施此限制。在外部系统中对组织控制的系统媒体的使用限制包括对媒体使用方式和条件的限制。要求可移动系统媒体具有可识别的所有者(例如个人、组织或项目)可降低使用此类技术的风险，使组织能够分配责任和问责，以解决媒体中的已知漏洞(例如插入恶意代码)。

参考文献

源控制：MP-07

支持性出版物：SP 800-111[51]

03.08.08 Withdrawn

Incorporated into 03.08.07.

03.08.09 System Backup – Cryptographic Protection

a. Protect the confidentiality of backup information.

b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.

DISCUSSION

The selection of cryptographic mechanisms is based on the need to protect the confidentiality of backup information. Hardware security module (HSM) devices safeguard and manage cryptographic keys and provide cryptographic processing. Cryptographic operations (e.g., encryption, decryption, and signature generation and verification) are typically hosted on the HSM device, and many implementations provide hardware-accelerated mechanisms for cryptographic operations. This requirement is related to 03.13.11.

REFERENCES

Source Controls: CP-09, CP-09(08)

Supporting Publications: SP 800-34 [52], SP 800-130 [53], SP 800-152 [54]

3.9. Personnel Security

03.09.01 Personnel Screening

a. Screen individuals prior to authorizing access to the system.

b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening*].

DISCUSSION

Personnel security screening activities involve the assessment of the conduct, integrity, judgment, loyalty, reliability, and stability of an individual (i.e., the individual's trustworthiness) prior to authorizing access to the system or when elevating system access. The screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and criteria established for the level of access required for the assigned position.

03.08.08 已撤回

已纳入03.08.07。

03.08.09 系统备份 - 加密保护

a. 保护备份信息的机密性。

b. 实施加密机制，防止在备份存储位置未经授权披露CUI。

讨论

密码机制的选择基于保护备份信息保密性的需要。硬件安全模块(HSM)设备保护和管理的密码密钥并提供密码处理。密码操作(例如加密、解密以及签名生成和验证)通常托管在HSM设备上，许多实现为密码操作提供硬件加速机制。本要求与03.13.11相关。

参考文献

源控制：CP-09、CP-09(08)

支持性出版物：SP 800-34[52]、SP 800-130[53]、SP 800-152[54]

3.9. 人员安全

03.09.01 人员筛查

a.在授权访问系统之前对个人进行筛查。b.按照[赋值：组织定义的需重新筛查的条件]对个人进行重新筛查。

讨论

人员安全筛查活动涉及在授权访问系统之前或提升系统访问权限时，对个人的行为、完整性、判断力、忠诚度、可靠性和稳定性(即个人的可信度)进行评估。筛查和重新筛查活动反映适用的联邦法律、行政命令、指令、政策、法规以及为所分配职位所需访问级别建立的标准。

REFERENCES

Source Control: PS-03

Supporting Publications: SP 800-181 [34]

03.09.02 Personnel Termination and Transfer

a. When individual employment is terminated:
   1. Disable system access within [*Assignment: organization-defined time period*],
   2. Terminate or revoke authenticators and credentials associated with the individual, and
   3. Retrieve security-related system property.
b. When individuals are reassigned or transferred to other positions in the organization:
   1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and
   2. Modify access authorization to correspond with any changes in operational need.

DISCUSSION

Security-related system property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that accountability is achieved for the organizational property. Security topics at exit interviews include reminding individuals of potential limitations on future employment and non-disclosure agreements. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment.

The timely execution of termination actions is essential for individuals who have been terminated for cause. Organizations may consider disabling the accounts of individuals who are being terminated prior to the individuals being notified. This requirement applies to the reassignment or transfer of individuals when the personnel action is permanent or of such extended duration as to require protection. Protections that may be required for transfers or reassignments to other positions within organizations include returning old and issuing new identification cards, keys, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing access to official records to which individuals had access at previous work locations in previous system accounts.

参考文献

源控制：PS-03

支持性出版物：SP 800-181[34]

03.09.02 人员解雇与调动

a. 当个人雇佣关系终止时：
   1. 在[赋值：组织定义的时间段]内禁用系统访问，
   2. 终止或撤销与该个人相关的身份验证器和凭证，以及
   3. 检索与安全相关的系统属性。
b. 当个人被重新分配或转移到组织中的其他职位时：
   1. 审查并确认当前对系统和设施的逻辑和物理访问授权的持续运营需求，以及
   2. 修改访问授权，使其与运行需求的任何变化保持一致。

讨论

安全相关的系统财产包括硬件身份验证令牌、系统管理技术手册、密钥、身份证件和建筑通行证。离职面谈确保被解雇人员了解作为前员工所承受的安全约束，并实现对组织财产的问责。离职面谈中的安全主题包括提醒个人未来就业的潜在限制和保密协议。对于某些个人，离职面谈可能并不总是可行的，包括与主管不在、疾病或擅自离岗相关的情况。

及时执行解雇操作对于因故被解雇的人员至关重要。组织可以考虑在通知个人之前禁用被解雇人员的账户。本要求适用于人员的重新分配或调动，当人事行动是永久性的或持续时间较长而需要保护时。调动或重新分配到组织内其他职位可能需要的保护包括归还旧的和发放新的身份证件、密钥和建筑通行证；更改系统访问授权(即特权)；关闭系统账户并建立新账户；以及提供对个人在以前工作地点以前系统账户中可访问的官方记录的访问。

REFERENCES

Source Controls: PS-04, PS-05

Supporting Publications: None

3.10. Physical Protection

03.10.01 Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.

b. Issue authorization credentials for facility access.

c. Review the facility access list [*Assignment: organization-defined frequency*].

d. Remove individuals from the facility access list when access is no longer required.

DISCUSSION

A facility can include one or more physical locations containing systems or system components that process, store, or transmit CUI. Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include identification badges, identification cards, and smart cards. Organizations determine the strength of the authorization credentials consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

REFERENCES

Source Control: PE-02

Supporting Publications: None

03.10.02 Monitoring Physical Access

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.

b. Review physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*].

参考文献

源控制：PS-04、PS-05

支持性出版物：无

3.10. 物理保护

03.10.01 物理访问授权

a. 制定、批准并维护有权访问系统所在设施的个人名单。

b. 为设施访问签发授权凭证。

c. 按照[赋值：组织定义的频率]审查设施访问名单。

d. 当不再需要访问权限时，将个人从设施访问名单中移除。

讨论

设施可以包括一个或多个物理位置，其中包含处理、存储或传输CUI的系统或系统组件。物理访问授权适用于员工和访客。拥有永久物理访问授权凭证的个人不被视为访客。授权凭证包括身份徽章、身份证件和智能卡。组织根据适用的法律、行政命令、指令、法规、政策、标准和指南确定授权凭证的强度。对于设施内被指定为可公开访问的某些区域，可能不需要物理访问授权。

参考文献

源控制：PE-02

支持性出版物：无

03.10.02 监控物理访问

a. 监控对系统所在设施的物理访问，以检测和响应物理安全事件。

b. 按照[赋值：组织定义的频率]以及在发生[赋值：组织定义的事件或事件的潜在迹象]时，审查物理访问日志。

DISCUSSION

A facility can include one or more physical locations containing systems or system components that process, store, or transmit CUI. Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help to identify suspicious activities, anomalous events, or potential threats. The reviews can be supported by audit logging controls if the access logs are part of an automated system. Incident response capabilities include investigations of physical security incidents and responses to those incidents. Incidents include security violations or suspicious physical access activities, such as access outside of normal work hours, repeated access to areas not normally accessed, access for unusual lengths of time, and out-of-sequence access.

REFERENCES

Source Control: PE-06

Supporting Publications: None

03.10.03 Withdrawn

Incorporated into 03.10.07.

03.10.04 Withdrawn

Incorporated into 03.10.07.

03.10.05 Withdrawn

Incorporated into 03.10.07.

03.10.06 Alternate Work Site

a. Determine alternate work sites allowed for use by employees.

b. Employ the following security requirements at alternate work sites: [*Assignment: organization-defined security requirements*].

DISCUSSION

Alternate work sites include the private residences of employees or other facilities designated by the organization. Alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different security requirements for specific alternate work sites or types of sites, depending on the work-related activities conducted at the sites. Assessing the

讨论

设施可以包括一个或多个物理位置，其中包含处理、存储或传输CUI的系统或系统组件。物理访问监控包括组织设施内的可公开访问区域。物理访问监控的示例包括警卫、视频监控设备(即摄像头)和传感器设备。审查物理访问日志有助于识别可疑活动、异常事件或潜在威胁。如果访问日志是自动化系统的一部分，审查可以得到审计日志记录控制的支持。事件响应能力包括对物理安全事件的调查和对这些事件的响应。事件包括安全违规或可疑的物理访问活动，例如在正常工作时间之外访问、反复访问通常不访问的区域、访问时间异常长以及乱序访问。

参考文献

源控制：PE-06

支持性出版物：无

03.10.03 已撤回

已纳入03.10.07。

03.10.04 已撤销

已纳入03.10.07。

03.10.05 已撤回

已纳入03.10.07。

03.10.06 备用工作场所

a. 确定允许员工使用的备用工作地点。

b. 在备用工作场所采用以下安全要求：[赋值：组织定义的安全要求]。

讨论

备用工作场所包括员工的私人住所或组织指定的其他设施。备用工作场所可以在应急操作期间提供随时可用的备用地点。组织可以根据场所进行的工作相关活动，为特定备用工作场所或场所类型定义不同的安全要求。评估

effectiveness of the requirements and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

REFERENCES

Source Control: PE-17

Supporting Publications: SP 800-46 [14], SP 800-114 [20]

03.10.07 Physical Access Control

a. Enforce physical access authorizations at entry and exit points to the facility where the system resides by:
   1. Verifying individual physical access authorizations before granting access to the facility and
   2. Controlling ingress and egress with physical access control systems, devices, or guards.
b. Maintain physical access audit logs for entry or exit points.
c. Escort visitors, and control visitor activity.
d. Secure keys, combinations, and other physical access devices.
e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.

DISCUSSION

This requirement addresses physical locations containing systems or system components that process, store, or transmit CUI. Organizations determine the types of guards needed, including professional security staff or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include exterior access points, interior access points to systems that require supplemental access controls, or both. Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors.

Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and only allowing access to authorized individuals, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, facsimile machines, audio devices, and copiers.

要求的有效性并提供在备用工作场所沟通事件的手段，支持组织的应急计划活动。

参考文献

源控制：PE-17

支持性出版物：SP 800-46[14],SP 800-114[20]

03.10.07 物理访问控制

a. 通过以下方式在系统所在设施的入口和出口点执行物理访问授权：
   1. 在授予设施访问权限之前验证个人物理访问授权，以及
   2. 使用物理访问控制系统、设备或警卫控制进出。
b. 维护进出点的物理访问审计日志。
c. 陪同访客，并控制访客活动。
d. 保护密钥、密码组合及其他物理访问设备。
e. 控制对输出设备的物理访问，防止未经授权的个人获取CUI。

讨论

本要求涉及包含处理、存储或传输CUI的系统或系统组件的物理位置。组织确定所需警卫的类型，包括专业安保人员或行政人员。物理访问设备包括钥匙、锁、密码组合、生物识别读取器和读卡器。物理访问控制系统符合适用的法律、行政命令、指令、政策、法规、标准和指南。组织在所使用的审计日志类型方面具有灵活性。审计日志可以是程序性的、自动化的或两者的某种组合。物理访问点可以包括外部访问点、需要补充访问控制的系统内部访问点，或两者兼有。物理访问控制适用于员工和访客。拥有永久物理访问授权的个人不被视为访客。

控制对输出设备的物理访问包括将输出设备放置在带键盘或读卡器访问控制的锁定房间或其他安全区域中，仅允许授权个人访问，将输出设备放置在可由人员监控的位置，安装显示器或屏幕过滤器，以及使用耳机。输出设备的示例包括显示器、打印机、扫描仪、传真机、音频设备和复印机。

REFERENCES

Source Controls: PE-03, PE-05

Supporting Publications: None

03.10.08 Access Control for Transmission

Control physical access to system distribution and transmission lines within organizational facilities.

DISCUSSION

Safeguarding measures applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such measures may also be necessary to prevent eavesdropping or the modification of unencrypted transmissions. Safeguarding measures used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, cabling protection with conduit or cable trays, and wiretapping sensors.

REFERENCES

Source Control: PE-04

Supporting Publications: None

3.11. Risk Assessment

03.11.01 Risk Assessment

a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.

b. Update risk assessments [*Assignment: organization-defined frequency*].

DISCUSSION

Establishing the system boundary is a prerequisite to assessing the risk of the unauthorized disclosure of CUI. Risk assessments consider threats, vulnerabilities, likelihood, and adverse impacts to organizational operations and assets based on the operation and use of the system and the unauthorized disclosure of CUI. Risk assessments also consider risks from external parties (e.g., contractors operating systems on behalf of the organization, service providers, individuals accessing systems, and outsourcing entities). Risk assessments can be conducted at the organization level, the mission or business process level, or the system level and at any phase in the system development life cycle. Risk assessments include supply

参考文献

源控制：PE-03、PE-05

支持性出版物：无

03.10.08 传输访问控制

控制对组织设施内系统分布和传输线路的物理访问。

讨论

应用于系统分布和传输线路的保护措施防止意外损坏、中断和物理篡改。此类措施也可能有必要用于防止窃听或修改未加密的传输。用于控制对系统分布和传输线路物理访问的保护措施包括断开或锁定的备用插孔、锁定的配线柜、使用导管或电缆桥架的布线保护以及窃听传感器。

参考文献

源控制：PE-04

支持性出版物：无

3.11. 风险评估

03.11.01 风险评估

a. 评估因处理、存储或传输CUI而导致的未经授权披露的风险(包括供应链风险)。

b. 按照[赋值：组织定义的频率]更新风险评估。

讨论

建立系统边界是评估CUI未经授权披露风险的前提条件。风险评估考虑威胁、脆弱性、可能性以及对组织运营和资产的不利影响，基于系统的运行和使用以及CUI的未经授权披露。风险评估还考虑来自外部的风险(例如，代表组织运行系统的承包商、服务提供商、访问系统的个人以及外包实体)。风险评估可以在组织层面、任务或业务流程层面或系统层面进行，并可在系统开发生命周期的任何阶段进行。风险评估包括供应

chain-related risks associated with suppliers or contractors and the system, system component, or system service that they provide.

REFERENCES

Source Controls: RA-03, RA-03(01), SR-06

Supporting Publications: SP 800-30 [55], SP 800-161 [33]

03.11.02 Vulnerability Monitoring and Scanning

a. Monitor and scan the system for vulnerabilities [*Assignment: organization-defined frequency*] and when new vulnerabilities affecting the system are identified.

b. Remediate system vulnerabilities within [*Assignment: organization-defined response times*].

c. Update system vulnerabilities to be scanned [*Assignment: organization-defined frequency*] and when new vulnerabilities are identified and reported.

DISCUSSION

Organizations determine the required vulnerability scanning for system components and ensure that potential sources of vulnerabilities (e.g., networked printers, scanners, and copiers) are not overlooked. Vulnerability analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, or binary analysis. Organizations can use these approaches in source code reviews and tools (e.g., static analysis tools, web-based application scanners, binary analyzers). Vulnerability scanning includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating flow control mechanisms.

To facilitate interoperability, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention. Sources for vulnerability information also include the Common Weakness Enumeration (CWE) listing, the National Vulnerability Database (NVD), and the Common Vulnerability Scoring System (CVSS).

REFERENCES

Source Controls: RA-05, RA-05(02)

Supporting Publications: SP 800-40 [56], SP 800-53A [57], SP 800-70 [44], SP 800-115 [58], SP 800-126 [45]

与供应商或承包商及其提供的系统、系统组件或系统服务相关的供应链风险。

参考文献

源控制：RA-03、RA-03(01)、SR-06

支持性出版物：SP 800-30[55],SP 800-161[33]

03.11.02 漏洞监控与扫描

a. 按照[赋值：组织定义的频率]以及在识别出影响系统的新脆弱性时，监控和扫描系统以发现脆弱性。

b. 在[赋值：组织定义的响应时间]内修复系统脆弱性。

c. 按照[赋值：组织定义的频率]以及在识别和报告新脆弱性时，更新要扫描的系统脆弱性。

讨论

组织确定系统组件所需的脆弱性扫描，并确保潜在的脆弱性来源(例如，网络打印机、扫描仪和复印机)不被忽视。对定制软件的脆弱性分析可能需要额外的方法，例如静态分析、动态分析或二进制分析。组织可以在源代码审查和工具(例如，静态分析工具、基于Web的应用程序扫描器、二进制分析器)中使用这些方法。脆弱性扫描包括扫描补丁级别；扫描不应被用户或设备访问的功能、端口、协议和服务；以及扫描配置不当或运行不正确的流控制机制。

为促进互操作性，组织考虑使用以通用脆弱性与暴露(CVE)命名规范表达脆弱性的扫描工具。脆弱性信息的来源还包括通用弱点枚举(CWE)列表、国家脆弱性数据库(NVD)以及通用脆弱性评分系统(CVSS)。

参考文献

源控制：RA-05、RA-05(02)

支持性出版物：SP 800-40[56]、SP 800-53A[57]、SP 800-70[44]、SP 800-115 [58]，SP 800-126 [45]

03.11.03 Withdrawn

Incorporated into 03.11.02.

03.11.04 Risk Response

Respond to findings from security assessments, monitoring, and audits.

DISCUSSION

This requirement addresses the need to determine an appropriate response to risk before generating a plan of action and milestones (POAM) entry. It may be possible to mitigate the risk immediately so that a POAM entry is not needed. However, a POAM entry is generated if the risk response is to mitigate the identified risk and the mitigation cannot be completed immediately.

REFERENCES

Source Control: RA-07

Supporting Publications: SP 800-30 [55], SP 800-37 [59], SP 800-39 [60], SP 800-160-1 [11]

3.12. Security Assessment and Monitoring

03.12.01 Security Assessment

Assess the security requirements for the system and its environment of operation [*Assignment: organization-defined frequency*] to determine if the requirements have been satisfied.

DISCUSSION

By assessing the security requirements, organizations determine whether the necessary safeguards and countermeasures are implemented correctly, operating as intended, and producing the desired outcome. Security assessments identify weaknesses in the system and provide the essential information needed to make risk-based decisions. Security assessment reports document assessment results in sufficient detail as deemed necessary by the organization to determine the accuracy and completeness of the reports. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

REFERENCES

Source Control: CA-02

Supporting Publications: SP 800-53 [8], SP 800-53A [57], SP 800-37 [59], SP 800-115 [58]

03.11.03 已撤回

已纳入03.11.02。

03.11.04 风险应对

响应安全评估、监控和审计的发现。

讨论

本要求涉及在生成行动计划与里程碑(POAM)条目之前确定对风险的适当响应的必要性。可能可以立即缓解风险，从而不需要POAM条目。然而，如果风险响应是缓解已识别的风险且缓解无法立即完成，则生成POAM条目。

参考文献

源控制：RA-07

支持性出版物：SP 800-30[55]、SP 800-37[59]、SP 800-39[60]、SP 800-160-1[11]

3.12. 安全评估与监控

03.12.01 安全评估

评估系统及其运行环境的安全要求[赋值：组织定义的频率]，以确定这些要求是否已得到满足。

讨论

通过评估安全要求，组织确定必要的保障措施和对策是否被正确实施、按预期运行并产生期望的结果。安全评估识别系统中的弱点，并提供做出基于风险的决策所需的基本信息。安全评估报告以组织认为必要的足够详细程度记录评估结果，以确定报告的准确性和完整性。安全评估结果提供给适合所进行评估类型的个人或角色。

参考文献

源控制：CA-02

支持性出版物：SP 800-53[8]、SP 800-53A[57]、SP 800-37[59]、SP 800-115 [58]

03.12.02 Plan of Action and Milestones

a. Develop a plan of action and milestones for the system:
   1. To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and
   2. To reduce or eliminate known system vulnerabilities.
b. Update the existing plan of action and milestones based on the findings from:
   1. Security assessments,
   2. Audits or reviews, and
   3. Continuous monitoring activities.

DISCUSSION

Plans of action and milestones (POAMs) are important documents in organizational security programs. Organizations use POAMs to describe how unsatisfied security requirements will be met and how planned mitigations will be implemented. Organizations can document system security plans and POAMs as separate or combined documents in any format. Federal agencies may consider system security plans and POAMs as inputs to risk-based decisions on whether to process, store, or transmit CUI on a system hosted by a nonfederal organization.

REFERENCES

Source Control: CA-05

Supporting Publications: SP 800-37 [59]

03.12.03 Continuous Monitoring

Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.

DISCUSSION

Continuous monitoring at the system level facilitates ongoing awareness of the system security posture to support risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess and monitor their systems at a frequency that is sufficient to support risk-based decisions. Different types of security requirements may require different monitoring frequencies.

REFERENCES

Source Control: CA-07

Supporting Publications: SP 800-37 [59], SP 800-39 [60], SP 800-53A [57], SP 800-115 [58], SP 800-137 [49]

03.12.02 行动计划与里程碑

a. 为系统制定行动计划和里程碑：
   1. 记录计划中的补救措施，以纠正安全评估期间发现的弱点或缺陷，以及
   2. 降低或消除已知的系统漏洞。
b. 根据以下发现更新现有的行动计划和里程碑：
   1. 安全评估，
   2. 审计或审查，以及
   3. 持续监控活动。

讨论

行动计划和里程碑(POAM)是组织安全计划中的重要文件。组织使用POAM来描述如何满足未满足的安全要求以及如何实施计划的缓解措施。组织可以将系统安全计划和POAM记录为任意格式的单独或合并文件。联邦机构可以将系统安全计划和POAM视为基于风险的决策的输入，这些决策涉及是否在由非联邦组织托管的系统上处理、存储或传输CUI。

参考文献

源控制：CA-05

支持性出版物：SP 800-37[59]

03.12.03 持续监控

制定并实施系统级持续监控策略，包括持续监控和安全评估。

讨论

系统级持续监控有助于持续了解系统安全态势，以支持风险管理决策。术语持续和*ongoing*意味着组织以足以支持基于风险的决策的频率评估和监控其系统。不同类型的安全要求可能需要不同的监控频率。

参考文献

源控制：CA-07

支持性出版物：SP 800-37[59]、SP 800-39[60]、SP 800-53A[57]、SP 800-115 [58]，SP 800-137 [49]

03.12.04 Withdrawn

Incorporated into 03.15.02.

03.12.05 Information Exchange

a. Approve and manage the exchange of CUI between the system and other systems using [*Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements*].

b. Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.

c. Review and update the exchange agreements [*Assignment: organization-defined frequency*].

DISCUSSION

Information exchange applies to information exchanges between two or more systems, both internal and external to the organization. Organizations consider the risks related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security requirements or policies. The types of agreements selected are based on factors such as the relationship between the organizations exchanging information (e.g., government to government, business to business, government to business, government or business, or government or business to individual) and the level of access to the organizational system by users of the other system. The types of agreements can include information exchange security agreements, interconnection security agreements, memoranda of understanding or agreement, service-level agreements, or other types of agreements.

Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal agencies and nonfederal organizations (e.g., service providers, contractors, system developers, and system integrators). The types of information contained in exchange agreements include the interface characteristics, security requirements, controls, and responsibilities for each system.

REFERENCES

Source Control: CA-03

Supporting Publications: SP 800-47 [83]

03.12.04 已撤回

已纳入03.15.02。

03.12.05 信息交换

a. 使用[选择*(一项或多项)*：互连安全协议；信息交换安全协议；谅解备忘录或协议；服务级别协议；用户协议；保密协议；其他类型的协议]批准并管理系统与其他系统之间的CUI交换。

b. 作为交换协议的一部分，记录每个系统的接口特征、安全要求和责任。

c. 审查并更新交换协议[赋值：组织定义的频率]。

讨论

信息交换适用于组织内部和外部两个或多个系统之间的信息交换。组织考虑当系统与可能具有不同安全要求或策略的其他系统交换信息时可能引入的新威胁或增加的威胁相关的风险。所选协议类型基于以下因素：交换信息的组织之间的关系(例如，政府与政府、企业与企业的、政府与企业、政府或企业、或政府或企业与个人)以及其他系统的用户对组织系统的访问级别。协议类型可以包括信息交换安全协议、互连安全协议、谅解备忘录或协议、服务级别协议或其他类型的协议。

组织可将协议信息纳入正式合同，特别是对于联邦机构与非联邦组织(例如服务提供商、承包商、系统开发人员和系统集成商)之间建立的信息交换。交换协议中包含的信息类型包括每个系统的接口特征、安全要求、控制措施和责任。

参考文献

源控制：CA-03

支持性出版物：SP 800-47[83]

3.13. System and Communications Protection

03.13.01 Boundary Protection

a. Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.

b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

c. Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.

DISCUSSION

Managed interfaces include gateways, routers, firewalls, network-based malicious code analysis, virtualization systems, and encrypted tunnels implemented within a security architecture. Subnetworks that are either physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses.

REFERENCES

Source Control: SC-07

Supporting Publications: SP 800-41 [64], SP 800-125B [65], SP 800-160-1 [11], SP 800-189 [67], SP 800-207 [66]

03.13.02 Withdrawn

Recategorized as NCO.

03.13.03 Withdrawn

Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.

03.13.04 Information in Shared System Resources

Prevent unauthorized and unintended information transfer via shared system resources.

3.13.系统与通信保护

03.13.01 边界防护

a. 监视并控制系统外部受管理接口和系统内关键内部受管理接口处的通信。

b. 为可公开访问的系统组件实现与内部网络在物理上或逻辑上分离的子网。

c. 仅通过由按照组织安全架构布置的边界保护设备组成的受管理接口连接到外部系统。

讨论

受管接口包括在安全架构内实施的网关、路由器、防火墙、基于网络的恶意代码分析、虚拟化系统和加密隧道。与内部网络在物理上或逻辑上隔离的子网络称为隔离区或DMZ。限制或禁止组织系统内的接口包括将外部Web流量限制到受管接口内的指定Web服务器、禁止看似欺骗内部地址的外部流量，以及禁止看似欺骗外部地址的内部流量。

参考文献

源控制：SC-07

支持性出版物：SP 800-41[64]、SP 800-125B[65]、SP 800-160-1[11]、SP 800-189[67]、SP 800-207[66]

03.13.02 已撤回

重新归类为NCO。

03.13.03 已撤回

由03.01.01、03.01.02、03.01.03、03.01.04、03.01.05、03.01.06和03.01.07处理。

03.13.04 共享系统资源中的信息

防止通过共享系统资源进行未经授权和意外的信息传输。

DISCUSSION

Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, the control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted, covert channels (including storage and timing channels) in which shared system resources are manipulated to violate information flow restrictions, or components within systems for which there are only single users or roles.

REFERENCES

Source Control: SC-04

Supporting Publications: None

03.13.05 Withdrawn

Incorporated into 03.13.01.

03.13.06 Network Communications – Deny by Default – Allow by Exception

Deny network communications traffic by default, and allow network communications traffic by exception.

DISCUSSION

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, allow-by-exception network communications traffic policy ensures that only essential and approved connections are allowed.

REFERENCES

Source Control: SC-07(05)

Supporting Publications: SP 800-41 [64], SP 800-77 [18], SP 800-189 [67]

03.13.07 Withdrawn

Addressed by 03.01.12, 03.04.02 and 03.04.06.

讨论

通过共享系统资源防止未经授权和意外的信息传输，可阻止由先前用户或角色(或代表先前用户或角色行事的进程)的操作所产生的信息，被在那些资源释放回系统之后获得共享系统资源访问权的当前用户或角色(或代表当前用户或角色行事的当前进程)所获取。共享系统资源中的信息也适用于信息的加密表示。在其他语境中，对共享系统资源中信息的控制被称为对象重用和残留信息保护。共享系统资源中的信息不涉及信息残留，即名义上已删除数据的残留表示；也不涉及隐蔽信道(包括存储信道和定时信道)，即操纵共享系统资源以违反信息流限制；也不涉及系统中仅有单一用户或角色的组件。

参考文献

源控制：SC-04

支持性出版物：无

03.13.05 已撤销

已纳入03.13.01。

03.13.06 网络通信 - 默认拒绝 - 例外允许

默认拒绝网络通信流量，并例外允许网络通信流量。

讨论

本要求适用于系统边界处和系统内已识别点处的入站和出站网络通信流量。拒绝所有、例外允许的网络通信流量策略确保仅允许必要且经批准的连接。

参考文献

源控制：SC-07(05)

支持性出版物：SP 800-41[64]、SP 800-77[18]、SP 800-189[67]

03.13.07 已撤销

由 03.01.12、03.04.02 和 03.04.06 处理。

03.13.08 Transmission and Storage Confidentiality

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.

DISCUSSION

This requirement applies to internal and external networks and any system components that can transmit CUI, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are susceptible to interception and modification. Encryption protects CUI from unauthorized disclosure during transmission and while in storage. Cryptographic mechanisms that protect the confidentiality of CUI during transmission include TLS and IPsec. Information in storage (i.e., information at rest) refers to the state of CUI when it is not in process or in transit and resides on internal or external storage devices, storage area network devices, and databases. Protecting CUI in storage does not focus on the type of storage device or the frequency of access to that device but rather on the state of the information. This requirement relates to 03.13.11.

REFERENCES

Source Controls: SC-08, SC-08(01), SC-28, SC-28(01)

Supporting Publications: FIPS 140-3 [38], FIPS 197 [68], SP 800-46 [14], SP 800-52 [69], SP 800-56A [73], SP 800-56B [74], SP 800-56C [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-111 [51], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-124 [28], SP 800-177 [70]

03.13.09 Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

DISCUSSION

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions includes deallocating TCP/IP addresses or port pairs at the operating system level or deallocating networking assignments at the application level if multiple application sessions are using a single network connection. Time periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

03.13.08 传输与存储保密性

实施加密机制，以防止CUI在传输期间和存储期间未经授权披露。

讨论

本要求适用于内部和外部网络以及任何可传输 CUI 的系统组件，包括服务器、笔记本电脑、台式计算机、移动设备、打印机、复印机、扫描仪、传真机和无线电设备。未受保护的通信路径易受拦截和修改。加密在传输期间和存储期间保护 CUI 免遭未经授权的泄露。在传输期间保护 CUI 保密性的密码机制包括 TLS 和 IPsec。存储中的信息(即静态信息)是指 CUI 不在处理中或传输中、而驻留在内部或外部存储设备、存储区域网络设备和数据库上时的状态。保护存储中的 CUI 并不关注存储设备的类型或对该设备的访问频率，而是关注信息的状态。本要求与03.13.11相关。

参考文献

源控制：SC-08、SC-08(01)、SC-28、SC-28(01)

支持性出版物：FIPS 140-3[38]、FIPS 197[68]、SP 800-46[14]、SP 800-52 [69]，SP 800-56A [73]，SP 800-56B [74]，SP 800-56C [75]，SP 800-57-1 [15]，SP 800-572 [16]，SP 800-57-3 [17]，SP 800-77 [18]，SP 800-111 [51]，SP 800-113 [19]，SP 800-114 [20]，SP 800-121 [21]，SP 800-124 [28]，SP 800-177 [70]

03.13.09 网络断开

在会话结束时或在[赋值：组织定义的时间段]不活动之后，终止与通信会话相关联的网络连接。

讨论

本要求适用于内部和外部网络。终止与通信会话相关联的网络连接包括在操作系统级别释放TCP/IP地址或端口对，或者如果多个应用程序会话正在使用单个网络连接，则在应用程序级别释放网络分配。不活动时间段可由组织确定，并包括按网络访问类型或特定网络访问的时间段。

REFERENCES

Source Control: SC-10

Supporting Publications: None

03.13.10 Cryptographic Key Establishment and Management

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

DISCUSSION

Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to 03.13.11.

REFERENCES

Source Control: SC-12

Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]

03.13.11 Cryptographic Protection

Implement the following types of cryptography to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. FIPS-validated cryptography is recommended for the protection of CUI.

REFERENCES

Source Control: SC-13

Supporting Publications: FIPS 140-3 [38]

参考文献

源控制： SC-10

支持性出版物：无

03.13.10 加密密钥建立与管理

按照以下密钥管理要求建立并管理系统中的加密密钥：[赋值：组织定义的密钥生成、分发、存储、访问和销毁要求]。

讨论

加密密钥可使用手动程序或由手动程序支持的自动化机制来建立和管理。组织按照适用的联邦法律、行政命令、政策、指令、法规和标准满足密钥建立和管理要求，这些法律、命令、政策、指令、法规和标准规定了适当的选项、级别和参数。本要求与03.13.11相关。

参考文献

源控制： SC-12

支持性出版物：FIPS 140-3 [38]，SP 800-56A [73]，SP 800-56B [74]，SP 80056C [75]，SP 800-57-1 [15]，SP 800-57-2 [16]，SP 800-57-3 [17]，SP 800-63-3 [27]

03.13.11 加密保护

实施以下类型的密码术以保护CUI的保密性：[赋值：组织定义的密码术类型]。

讨论

密码术按照适用的法律、行政命令、指令、法规、政策、标准和指南实施。建议使用经FIPS验证的密码术来保护CUI。

参考文献

源控制： SC-13

支持性出版物：FIPS 140-3[38]

03.13.12 Collaborative Computing Devices and Applications

a. Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*].

b. Provide an explicit indication of use to users physically present at the devices.

DISCUSSION

Collaborative computing devices include white boards, microphones, and cameras. Notebook computers, smartphones, display monitors, and tablets containing cameras and microphones are considered part of collaborative computing devices when conferencing software is in use. Indication of use includes notifying users (e.g., a pop-up menu stating that recording is in progress or that the microphone has been turned on) when collaborative computing devices are activated. Dedicated video conferencing systems, which typically rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded. Solutions to prevent device usage include webcam covers and buttons to disable microphones.

REFERENCES

Source Control: SC-15

Supporting Publications: None

03.13.13 Mobile Code

a. Define acceptable mobile code and mobile code technologies.

b. Authorize, monitor, and control the use of mobile code.

DISCUSSION

Mobile code includes software programs or parts of programs that are obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. Decisions regarding the use of mobile code are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, VBScript, and WebGL. Usage restrictions and implementation guidelines apply to the selection and use of mobile code installed on servers and downloaded and executed on individual workstations and devices, including notebook computers, smart phones, and smart devices. Mobile code policies and procedures address the actions taken to prevent the development, acquisition, and use of unacceptable mobile code within the system, including requiring mobile code to be digitally signed by a trusted source.

03.13.12 协作计算设备与应用程序

a. 禁止远程激活协作计算设备和应用程序，以下例外情况除外：[赋值：允许远程激活的组织定义的例外情况]。

b. 向物理上在场于设备处的用户提供明确的使用指示。

讨论

协作计算设备包括白板、麦克风和摄像头。当使用会议软件时，包含摄像头和麦克风的笔记本电脑、智能手机、显示器和平板电脑被视为协作计算设备的一部分。使用指示包括在协作计算设备被激活时通知用户(例如，弹出菜单说明正在录制或麦克风已打开)。专用视频会议系统通常依赖参与者之一呼叫或连接另一方来激活视频会议，不在此列。防止设备使用的解决方案包括网络摄像头遮盖和禁用麦克风的按钮。

参考文献

源控制：SC-15

支持性出版物：无

03.13.13 移动代码

a. 定义可接受的移动代码和移动代码技术。

b. 授权、监控并控制移动代码的使用。

讨论

移动代码包括从远程系统获取、跨网络传输并在本地系统上执行的软件程序或程序的一部分，而无需接收方明确安装或执行。关于使用移动代码的决策基于该代码在被恶意使用时对系统造成损害的可能性。移动代码技术包括 Java applet、JavaScript、HTML5、VBScript 和 WebGL。使用限制和实施指南适用于安装在服务器上以及下载并在单个工作站和设备(包括笔记本电脑、智能手机和智能设备)上执行的移动代码的选择和使用。移动代码策略和程序涉及为防止在系统内开发、获取和使用不可接受的移动代码而采取的行动，包括要求移动代码由可信来源进行数字签名。

REFERENCES

Source Control: SC-18

Supporting Publications: SP 800-28 [71]

03.13.14 Withdrawn

Technology-specific.

03.13.15 Session Authenticity

Protect the authenticity of communications sessions.

DISCUSSION

Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of the communications sessions in the ongoing identities of other parties and the validity of the transmitted information. Authenticity protection includes protecting against adversary-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

REFERENCES

Source Control: SC-23

Supporting Publications: SP 800-52 [69], SP 800-77 [18], SP 800-95 [72], SP 800-113 [19]

03.13.16 Withdrawn

Incorporated into 03.13.08.

3.14. System and Information Integrity

03.14.01 Flaw Remediation

a. Identify, report, and correct system flaws.

b. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates.

DISCUSSION

Organizations identify systems that are affected by announced software and firmware flaws, including potential vulnerabilities that result from those flaws, and report this information to designated personnel with information security

参考文献

源控制：SC-18

支持性出版物：SP 800-28[71]

03.13.14 已撤销

特定于技术。

03.13.15 会话真实性

保护通信会话的真实性。

讨论

保护会话真实性涉及会话层面的通信保护，而非数据包层面。此类保护为通信会话双方对其他方持续身份及所传输信息有效性的信心奠定基础。真实性保护包括防范对手中间人攻击、会话劫持以及向会话中插入虚假信息。

参考文献

源控制：SC-23

支持性出版物：SP 800-52[69]、SP 800-77[18]、SP 800-95[72]、SP 800-113 [19]

03.13.16 已撤回

已纳入03.13.08。

3.14. 系统与信息完整性

03.14.01 缺陷修复

a. 识别、报告并纠正系统缺陷。

b. 在更新发布后的[分配：组织定义的时间段]内安装与安全相关的软件和固件更新。

讨论

组织识别受已公布软件和固件缺陷影响的系统，包括这些缺陷导致的潜在漏洞，并将此信息报告给具有信息安全职责的指定人员

responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address the flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources (e.g., CWE or CVE databases) when remediating system flaws. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors, including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types.

REFERENCES

Source Control: SI-02

Supporting Publications: SP 800-39 [60], SP 800-40 [56], SP 800-128 [41]

03.14.02 Malicious Code Protection

a. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.

c. Configure malicious code protection mechanisms to:

1. Perform scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and

2. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.

DISCUSSION

Malicious code insertions occur through the exploitation of system vulnerabilities. Malicious code can be inserted into the system in a variety of ways, including email, the internet, and portable storage devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats, contained in compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code may be present in commercial off-the-shelf software and custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions. Periodic scans of the system and real-time scans of files from external sources as files are downloaded, opened, or executed can detect malicious code. Malicious code protection mechanisms can also monitor systems for anomalous or unexpected behaviors and take appropriate actions.

职责。与安全相关的更新包括补丁、服务包、热修复和防病毒签名。组织处理在安全评估、持续监控、事件响应活动和系统错误处理期间发现的缺陷。组织在修复系统缺陷时可以利用可用资源(例如 CWE 或 CVE 数据库)。组织定义的更新与安全相关的软件和固件的时间段可能因多种因素而异，包括更新的关键性(即与所发现缺陷相关的脆弱性的严重程度)。某些类型的缺陷修复可能比其他类型需要更多测试。

参考文献

源控制：SI-02

支持性出版物：SP 800-39[60]、SP 800-40[56]、SP 800-128[41]

03.14.02 恶意代码防护

a. 在系统入口和出口点实施恶意代码防护机制，以检测和清除恶意代码。

b. 按照配置管理策略和程序，在有新版本可用时更新恶意代码防护机制。

c. 将恶意代码防护机制配置为：

1. 1. 以[分配：组织定义的频率]对系统进行扫描，并在文件下载、打开或执行时对端点或系统入口和出口点来自外部来源的文件进行实时扫描；以及 2. 针对恶意代码检测结果，阻止恶意代码、隔离恶意代码或采取其他缓解措施。

讨论

恶意代码插入通过利用系统漏洞发生。恶意代码可以通过多种方式插入系统，包括电子邮件、互联网和便携式存储设备。恶意代码包括病毒、蠕虫、特洛伊木马和间谍软件。恶意代码可以以各种格式编码，包含在压缩或隐藏文件中，或使用隐写术等技术隐藏在文件中。恶意代码可能存在于商业现成软件和定制软件中，并可能包括逻辑炸弹、后门和其他类型的攻击，这些攻击可能影响组织的任务和业务功能。对系统进行定期扫描以及对来自外部源的文件在下载、打开或执行时进行实时扫描可以检测恶意代码。恶意代码保护机制还可以监控系统是否存在异常或意外行为并采取适当措施。

Malicious code protection mechanisms include signature- and non-signature-based technologies. Non-signature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Non-signature-based mechanisms include reputation-based technologies. Pervasive configuration management, anti-exploitation software, and software integrity controls may also be effective in preventing unauthorized code execution.

If malicious code cannot be detected by detection methods or technologies, organizations can rely on secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that the software only performs intended functions. Organizations may determine that different actions are warranted in response to the detection of malicious code. For example, organizations can define actions to be taken in response to the detection of malicious code during scans, malicious downloads, or malicious activity when attempting to open or execute files.

REFERENCES

Source Control: SI-03

Supporting Publications: SP 800-83 [76], SP 800-125B [65], SP 800-177 [70]

03.14.03 Security Alerts, Advisories, and Directives

a. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.

b. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.

DISCUSSION

There are many publicly available sources of system security alerts and advisories. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) generate security alerts and advisories to maintain situational awareness across the Federal Government and in nonfederal organizations. Software vendors, subscription services, and industry Information Sharing and Analysis Centers (ISACs) may also provide security alerts and advisories. Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations

恶意代码保护机制包括基于签名和非签名的技术。基于非签名的检测机制包括使用启发式的人工智能技术，以检测、分析和描述恶意代码的特征或行为，并为尚无签名或现有签名可能无效的此类代码提供控制。尚无有效签名或签名可能无效的恶意代码包括多态恶意代码(即复制时更改签名的代码)。基于非签名的机制包括基于信誉的技术。普遍配置管理、反利用软件和软件完整性控制也可能有效防止未经授权的代码执行。

如果恶意代码无法通过检测方法或技术检测到，组织可以依赖安全编码实践、配置管理和控制、可信采购流程以及监控实践来帮助确保软件仅执行预期功能。组织可以确定在检测到恶意代码时需要采取不同的行动。例如，组织可以定义在扫描、恶意下载或尝试打开或执行文件时的恶意活动中检测到恶意代码时应采取的行动。

参考文献

源控制：SI-03

支持性出版物：SP 800-83[76]、SP 800-125B[65]、SP 800-177[70]

03.14.03 安全警报、公告和指令

a. 持续接收来自外部组织的系统安全警报、公告和指令。

b. 根据需要生成并分发内部系统安全警报、公告和指令。

讨论

有许多公开可用的系统安全警报和公告来源。国土安全部网络安全和基础设施安全局(CISA)、国家安全局(NSA)和联邦调查局(FBI)生成安全警报和公告，以保持联邦政府和非联邦组织中的态势感知。软件供应商、订阅服务和行业信息共享与分析中心(ISAC)也可能提供安全警报和公告。遵守安全指令至关重要，因为许多此类指令具有关键性质，并且可能对组织运营产生潜在的即时不利影响

and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

REFERENCES

Source Control: SI-05

Supporting Publications: SP 800-161 [33]

03.14.04 Withdrawn

Incorporated into 03.14.02.

03.14.05 Withdrawn

Addressed by 03.14.02.

03.14.06 System Monitoring

a. Monitor the system to detect:
   1. Attacks and indicators of potential attacks and
   2. Unauthorized connections.

b. Identify unauthorized use of the system.

c. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.

DISCUSSION

System monitoring involves external and internal monitoring. Internal monitoring includes the observation of events that occur within the system. External monitoring includes the observation of events that occur at the system boundary. Organizations can monitor the system by observing audit record activities in real time or by observing other system aspects, such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events.

A system monitoring capability is achieved through a variety of tools and techniques (e.g., audit record monitoring software, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms that support critical applications with such devices being employed at managed system interfaces. The granularity of monitoring the information collected is based on organizational monitoring objectives and the capability of the system to support such objectives.

以及资产、个人、其他组织和国家(若指令未及时实施)。

参考文献

源控制：SI-05

支持性出版物：SP 800-161[33]

03.14.04 已撤回

已纳入03.14.02。

03.14.05 已撤回

由03.14.02处理。

03.14.06 系统监控

a. 监控系统以检测：
   1. 攻击与潜在攻击的迹象以及
   2. 未经授权的连接。

b.识别对系统的未经授权使用。c.监控入站和出站通信流量，以检测异常或未经授权的活动或状况。

讨论

系统监控涉及外部监控和内部监控。内部监控包括观察系统内发生的事件。外部监控包括观察系统边界处发生的事件。组织可以通过实时观察审计记录活动或观察其他系统方面(如访问模式、访问特征和其他操作)来监控系统。监控目标可指导事件的确定。

系统监控能力通过各种工具和技术(例如审计记录监控软件、入侵检测系统、入侵防御系统、恶意代码保护软件、扫描工具、网络监控软件)实现。监控设备的战略位置包括选定的边界位置和支持关键应用的服务器群附近，此类设备部署在受管理的系统接口处。监控所收集信息的粒度基于组织监控目标和系统支持此类目标的能力。

Systems connections can be network, remote, or local. A network connection is any connection with a device that communicates through a network (e.g., local area network, the internet). A remote connection is any connection with a device that communicates through an external network (e.g., the internet). Network, remote, and local connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in the system or propagating among system components, the unauthorized export of information, or signaling to external systems. Evidence of malicious code is used to identify a potentially compromised system. System monitoring requirements, including the need for types of system monitoring, may be referenced in other requirements.

REFERENCES

Source Controls: SI-04, SI-04(04)

Supporting Publications: SP 800-61 [47], SP 800-83 [76], SP 800-92 [35], SP 800-94 [29], SP 800-137 [49], SP 800-177 [70]

03.14.07 Withdrawn

Incorporated into 03.14.06.

03.14.08 Information Management and Retention

Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

DISCUSSION

Federal agencies consider data retention requirements for nonfederal organizations. Retaining CUI on nonfederal systems after contracts or agreements have concluded increases the attack surface for those systems and the risk of the information being compromised. NARA provides federal policy and guidance on records retention and schedules.

REFERENCES

Source Control: SI-12

Supporting Publications: None

系统连接可以是网络连接、远程连接或本地连接。网络连接是与通过网络(例如局域网、互联网)通信的设备的任何连接。远程连接是与通过外部网络(例如互联网)通信的设备的任何连接。网络连接、远程连接和本地连接可以是有线或无线的。

与入站和出站通信流量相关的不寻常或未经授权的活动或状况包括：表明系统内存在恶意代码或在系统组件间传播的内部流量、未经授权的信息导出，或向外部系统发送信号。恶意代码的证据用于识别可能已受损的系统。系统监控要求(包括对各类系统监控的需求)可能在其他要求中引用。

参考文献

源控制：SI-04、SI-04(04)

支持性出版物：SP 800-61[47]、SP 800-83[76]、SP 800-92[35]、SP 800-94 [29]，SP 800-137 [49]，SP 800-177 [70]

03.14.07 已撤回

已纳入03.14.06。

03.14.08 信息管理与保留

按照适用的法律、行政命令、指令、法规、政策、标准、指南和操作要求，管理和保留系统中的CUI以及系统输出的CUI。

讨论

联邦机构考虑非联邦组织的数据保留要求。在合同或协议结束后在非联邦系统上保留CUI会增加这些系统的攻击面以及信息被泄露的风险。NARA提供关于记录保留和保留期限表的联邦政策和指南。

参考文献

源控制：SI-12

支持性出版物：无

3.15. Planning

03.15.01 Policy and Procedures

a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.

b. Review and update policies and procedures [*Assignment: organization-defined frequency*].

DISCUSSION

This requirement addresses policies and procedures for the protection of CUI. Policies and procedures contribute to security assurance and should address each family of the CUI security requirements. Policies can be included as part of the organizational security policy or be represented by separate policies that address each family of security requirements. Procedures describe how policies are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security plans or in one or more separate documents.

REFERENCES

Source Controls: AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01, SR-01

Supporting Publications: SP 800-12 [61], SP 800-100 [62]

03.15.02 System Security Plan

a. Develop a system security plan that:

1. Defines the constituent system components;
2. Identifies the information types processed, stored, and transmitted by the system;
3. Describes specific threats to the system that are of concern to the organization;
4. Describes the operational environment for the system and any dependencies on or connections to other systems or system components;
5. Provides an overview of the security requirements for the system;
6. Describes the safeguards in place or planned for meeting the security requirements;
7. Identifies individuals that fulfill system roles and responsibilities; and

3.15. 规划

03.15.01 策略与程序

a. 制定、记录并向组织人员或角色分发满足CUI保护安全要求所需的策略和程序。

b. 审查和更新策略和程序[分配：组织定义的频率]。

讨论

本要求涉及保护 CUI 的策略和程序。策略和程序有助于安全保障，并应针对 CUI 安全要求的每个族。策略可作为组织安全策略的一部分，或由针对每个安全要求族的单独策略来体现。程序描述策略如何实施，可针对作为程序对象的个人或角色。程序可记录在系统安全计划中，或记录在一个或多个单独文档中。

参考文献

来源控制：AC-01、AT-01、AU-01、CA-01、CM-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PS-01、RA-01、SA-01、SC-01、SI-01、SR-01支持性出版物：SP 800-12[61]、SP 800-100[62]

03.15.02 系统安全计划

a. 制定一份系统安全计划，该计划应：

1. 定义组成系统的组件；
2. 识别系统处理、存储和传输的信息类型；
3. 描述组织关注的系统特定威胁；
4. 描述系统的运行环境以及对其他系统或系统组件的任何依赖或连接；
5. 概述系统的安全要求；
6. 描述为满足安全要求而已实施或计划实施的保障措施；
7. 识别履行系统角色和职责的个人；以及

8. Includes other relevant information necessary for the protection of CUI.

b. Review and update the system security plan [*Assignment: organization-defined frequency*].

c. Protect the system security plan from unauthorized disclosure.

DISCUSSION

System security plans provide key characteristics of the system that is processing, storing, and transmitting CUI and how the system and information are protected. System security plans contain sufficient information to enable a design and implementation that are unambiguously compliant with the intent of the plans and the subsequent determinations of risk if the plan is implemented as intended. System security plans can be a collection of documents, including documents that already exist. Effective system security plans reference policies, procedures, and documents (e.g., design specifications) that provide additional detailed information. This reduces the documentation requirements associated with security programs and maintains security information in other established management or operational areas related to enterprise architecture, the system development life cycle, systems engineering, and acquisition.

REFERENCES

Source Control: PL-02

Supporting Publications: SP 800-18 [63]

03.15.03 Rules of Behavior

a. Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.

b. Provide rules to individuals who require access to the system.

c. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.

d. Review and update the rules of behavior [*Assignment: organization-defined frequency*].

DISCUSSION

Rules of behavior represent a type of access agreement for system users. Organizations consider rules of behavior for the handling of CUI based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users.

8. 包括保护CUI所需的其他相关信息。

b. 审查和更新系统安全计划[分配：组织定义的频率]。

c. 保护系统安全计划免遭未经授权的披露。

讨论

系统安全计划提供处理、存储和传输 CUI 的系统的关键特征，以及系统和信息如何受到保护。系统安全计划包含足够的信息，使设计和实施能够明确符合计划的意图，以及在计划按预期实施时后续的风险判定。系统安全计划可以是文档的集合，包括已存在的文档。有效的系统安全计划引用提供额外详细信息的策略、程序和文档(例如设计规范)。这减少了与安全计划相关的文档要求，并将安全信息维护在与企业架构、系统开发生命周期、系统工程和采办相关的其他既定管理或运营领域中。

参考文献

源控制：PL-02

支持性出版物：SP 800-18[63]

03.15.03 **行为规则**

a. 制定规则，描述系统使用和保护CUI的责任及预期行为。

b. 向需要访问系统的个人提供规则。

c. 在授权访问CUI和系统之前，获得个人出具的书面确认，表明其已阅读、理解并同意遵守行为规则。

d. 审查和更新行为规则[分配：组织定义的频率]。

讨论

行为规则代表一种系统用户的访问协议。
组织根据个人用户角色和职责考虑CUI处理的行为规则，并区分适用于特权用户的规则和适用于一般用户的规则。

REFERENCES

Source Control: PL-04

Supporting Publications: SP 800-18 [63]

3.16. System and Services Acquisition

03.16.01 Security Engineering Principles

Apply the following systems security engineering principles to the development or modification of the system and system components: [*Assignment: organization-defined systems security engineering principles*].

DISCUSSION

Organizations apply systems security engineering principles to new development systems. For legacy systems, organizations apply systems security engineering principles to system modifications to the extent feasible, given the current state of hardware, software, and firmware components. The application of systems security engineering principles helps to develop trustworthy, secure, and resilient systems and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples include developing layered protections; establishing security policies, architectures, and controls as the foundation for system design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build trustworthy secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risks to acceptable levels; and make informed risk-management decisions.

REFERENCES

Source Control: SA-08

Supporting Publications: SP 800-160-1 [11], SP 800-160-2 [10], SP 800-207 [66]

03.16.02 Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.

参考文献

源控制：PL-04

支持性出版物：SP 800-18[63]

3.16. 系统和服务采购

03.16.01 安全工程原则

将以下系统安全工程原则应用于系统和系统组件的开发或修改：[分配：组织定义的系统安全工程原则]。

讨论

组织将系统安全工程原则应用于新开发系统。对于遗留系统，组织在给定硬件、软件和固件组件当前状态的情况下，在可行范围内将系统安全工程原则应用于系统修改。应用系统安全工程原则有助于开发可信、安全和有弹性的系统，并降低组织对中断、危害和威胁的易感性。示例包括：开发分层保护；建立安全策略、架构和控制作为系统设计的基础；将安全要求纳入系统开发生命周期；划定物理和逻辑安全边界；确保开发人员接受有关如何构建可信安全软件的培训；以及执行威胁建模以识别用例、威胁代理、攻击向量和模式、设计模式以及缓解风险所需的补偿控制。应用安全工程原则的组织可以促进可信、安全系统、系统组件和系统服务的开发；将风险降低到可接受水平；并做出知情的风险管理决策。

参考文献

源控制：SA-08

支持性出版物：SP 800-160-1[11]、SP 800-160-2[10]、SP 800-207[66]

03.16.02 不支持的系统组件

a. 当开发者、供应商或制造商不再提供组件支持时，更换系统组件。

b. 为无法更换的不受支持组件提供风险缓解选项或持续支持的替代来源。

DISCUSSION

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in opportunities for adversaries to exploit weaknesses or deficiencies in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities when newer technologies are unavailable or when the systems are so isolated that installing replacement components is not an option.

Alternative sources of support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational missions and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or obtain the services of external service providers who provide ongoing support for unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

REFERENCES

Source Control: SA-22

Supporting Publications: None

03.16.03 External System Services

a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [*Assignment: organization-defined security requirements*].

b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.

c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

DISCUSSION

External system services are provided by external service providers. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services

讨论

系统组件的支持包括软件补丁、固件更新、更换部件和维护合同。不支持组件的示例包括供应商不再提供关键软件补丁或产品更新的情况，这可能导致对手有机会利用已安装组件中的弱点或缺陷。更换不支持系统组件的例外情况包括：当较新技术不可用或系统隔离程度过高以致无法安装更换组件时，提供关键任务或业务能力的系统。

替代支持来源解决了当系统组件对组织任务和业务功能仍然至关重要时，为原始制造商、开发商或供应商不再支持的系统组件提供持续支持的需求。如有必要，组织可以通过为关键软件组件开发定制补丁来建立内部支持，或通过合同关系获得为不支持组件提供持续支持的外部服务提供商的服务。此类合同关系可以包括开源软件增值供应商。使用不支持系统组件的增加风险可以通过禁止此类组件连接到公共或不受控网络或实施其他形式的隔离来缓解。

参考文献

源控制：SA-22

支持性出版物：无

03.16.03 外部系统服务

a. 要求用于处理、存储或传输CUI的外部系统服务提供商遵守以下安全要求：[赋值：组织定义的安全要求]。

b. 定义并记录与外部系统服务相关的用户角色和职责，包括与外部服务提供商共担的职责。

c. 实施流程、方法和技术，以持续监控外部服务提供商对安全要求的合规情况。

讨论

外部系统服务由外部服务提供商提供。组织通过多种方式与外部服务提供商建立关系，包括业务合作伙伴关系、合同、机构间协议、业务线安排、许可协议、合资企业和供应链交换。管理使用外部系统服务所产生风险的责任

remains with the organization charged with protecting CUI. Service-level agreements define expectations of performance, describe measurable outcomes, and identify remedies, mitigations, and response requirements for instances of noncompliance. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when there is a need to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols. This requirement is related to 03.01.20.

REFERENCES

Source Control: SA-09

Supporting Publications: SP 800-160-1 [11], SP 800-161 [33]

3.17. Supply Chain Risk Management

03.17.01 Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.

b. Review and update the supply chain risk management plan [*Assignment: organization-defined frequency*].

c. Protect the supply chain risk management plan from unauthorized disclosure.

DISCUSSION

Dependence on the products, systems, and services of external providers and the nature of the relationships with those providers present an increasing level of risk to an organization. Threat actions that may increase security risks include unauthorized production, the insertion or use of counterfeits, tampering, poor manufacturing and development practices in the supply chain, theft, and the insertion of malicious software, firmware, and hardware. Supply chain risks can be endemic or systemic within a system, component, or service. Managing supply chain risks is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.

Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against the plans. The system-level SCRM plan is implementation-specific and provides constraints, policy implementation, requirements, and implications. It can either be stand-alone or

仍由负责保护CUI的组织承担。服务级别协议定义了性能期望，描述了可衡量的结果，并确定了不合规情况的补救措施、缓解措施和响应要求。来自外部服务提供商的关于在提供此类服务中使用的特定功能、端口、协议和服务的信息，在需要了解限制某些功能和服务或阻止某些端口和协议的权衡时可能有用。此要求与03.01.20相关。

参考文献

源控制：SA-09

支持性出版物：SP 800-160-1[11]、SP 800-161[33]

3.17. 供应链风险管理

03.17.01 供应链风险管理计划

a. 制定计划，以管理与系统、系统组件或系统服务的研究与开发、设计、制造、采购、交付、集成、运行、维护和处置相关的供应链风险。

b. 审查并更新供应链风险管理计划[赋值：组织定义的频率]。

c. 保护供应链风险管理计划免遭未经授权的披露。

讨论

对外部提供商的产品、系统和服务的依赖以及与这些提供商关系的性质给组织带来了日益增加的风险水平。可能增加安全风险的威胁行为包括未经授权的生产、插入或使用假冒产品、篡改、供应链中不良的制造和开发实践、盗窃以及插入恶意软件、固件和硬件。供应链风险可能是系统、组件或服务内的地方性或系统性风险。管理供应链风险是一项复杂的、多方面的工作，需要整个组织协调努力以建立信任关系并与内部和外部利益相关方沟通。

供应链风险管理(SCRM)活动包括识别和评估风险、确定适当的风险应对行动、制定SCRM计划以记录应对行动，以及对照计划监控绩效。系统级SCRM计划是特定于实施的，并提供约束、策略实施、要求和影响。它可以是独立的，也可以

incorporated into system security plans. The SCRM plan addresses the management, implementation, and monitoring of SCRM requirements and the development or sustainment of systems across the system development life cycle to support mission and business functions. Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to individual program, organizational, and operational contexts.

REFERENCES

Source Control: SR-02

Supporting Publications: SP 800-30 [55], SP 800-39 [60], SP 800-161 [33], SP 800-181 [34]

03.17.02 Acquisition Strategies, Tools, and Methods

Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

DISCUSSION

The acquisition process provides an important vehicle for protecting the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind purchases, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, the insertion of counterfeits, the insertion of malicious software or backdoors, and poor development practices throughout the system life cycle.

Organizations also consider providing incentives for suppliers to implement safeguards, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risks, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security requirements of the organization. Contracts may specify documentation protection requirements.

REFERENCES

Source Control: SR-05

Supporting Publications: SP 800-30 [55], SP 800-161 [33]

纳入系统安全计划。SCRM计划涉及SCRM要求的管理、实施和监控，以及在整个系统开发生命周期中开发或维持系统，以支持任务和业务功能。由于供应链在组织之间和组织内部可能存在显著差异，SCRM计划针对各个项目、组织和运营环境进行定制。

参考文献

源控制：SR-02

支持性出版物：SP 800-30[55]、SP 800-39[60]、SP 800-161[33]、SP 800-181 [34]

03.17.02 采购策略、工具和方法

制定并实施采购策略、合同工具和采购方法，以识别、防范和缓解供应链风险。

讨论

采购过程是保护供应链的重要工具。有许多有用的工具和技术可用，包括模糊系统或系统组件的最终用途、使用盲购、要求防篡改包装或使用可信或受控分销。供应链风险评估的结果可以为最适合情况的策略、工具和方法提供信息。工具和技术可以在整个系统生命周期内提供针对未经授权的生产、盗窃、篡改、插入假冒产品、插入恶意软件或后门以及不良开发实践的保护。

组织还应考虑为供应商提供激励措施以实施保障措施，促进其流程和安全实践的透明度，提供涉及禁止受污染或假冒组件的合同语言，并限制从不值得信赖的供应商处采购。组织应考虑为人员提供有关供应链风险、可用的缓解策略以及何时应采用这些计划的培训、教育和意识计划。审查和保护开发计划、文档和证据的方法应与组织的安全要求相称。合同可规定文档保护要求。

参考文献

源控制：SR-05

支持性出版物：SP 800-30[55],SP 800-161[33]

03.17.03 Supply Chain Requirements and Processes

a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.

b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [*Assignment: organization-defined security requirements*].

DISCUSSION

Supply chain elements include organizations, entities, or tools that are employed for the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, firmware, and systems development processes; shipping and handling procedures; physical security programs; personnel security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance, and disposal of systems and system components. Supply chain elements and processes are provided by organizations, system integrators, or external service providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to harm the organization and affect its ability to carry out its core missions or business functions.

REFERENCES

Source Control: SR-03

Supporting Publications: SP 800-30 [55], SP 800-161 [33]

03.17.03 供应链要求与流程

a. 建立流程，以识别和解决供应链要素和流程中的弱点或缺陷。

b. 执行以下安全要求，以防范系统、系统组件或系统服务面临的供应链风险，并限制供应链相关事件造成的危害或后果：[赋值：组织定义的安全要求]。

讨论

供应链要素包括用于系统及系统组件的研究、开发、设计、制造、采购、交付、集成、运行、维护和处置的组织、实体或工具。供应链流程包括硬件、软件、固件和系统开发流程；运输和处理程序；物理安全计划；人员安全计划；用于维护来源的配置管理工具、技术和方法；或与系统及系统组件的开发、采购、维护和处置相关的其他计划、流程或程序。供应链要素和流程由组织、系统集成商或外部服务提供商提供。供应链要素或流程中的弱点或缺陷代表潜在的漏洞，对手可利用这些漏洞来损害组织并影响其执行核心任务或业务功能的能力。

参考文献

源控制：SR-03

支持性出版物：SP 800-30[55],SP 800-161[33]

References

[1] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010. Available at https://www.govinfo.gov/app/details/DCPD-201000942

[2] Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009. Available at https://www.govinfo.gov/app/details/DCPD-200901022

[3] Atomic Energy Act (P.L. 83-703), August 1954. Available at https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919

[4] National Archives and Records Administration (2019) Controlled Unclassified Information (CUI) Registry. Available at https://www.archives.gov/cui

[5] 32 CFR Part 2002 (2016), Controlled Unclassified Information (CUI), September 2016. Available at https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf

[6] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[7] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[8] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[9] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[10] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[11] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[12] Joint Task Force (2020) Control Baselines for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[13] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

参考文献

[1] 第13556号行政命令(2010)受控非机密信息。(白宫，华盛顿特区),DCPD-201000942,2010年11月4日。可查阅https://www.govinfo.gov/app/details/DCPD-201000942

[2] 第13526号行政命令(2009)国家安全机密信息。(白宫，华盛顿特区),DCPD-200901022,2009年12月29日。可查阅https://www.govinfo.gov/app/details/DCPD-200901022

[3] 原子能法(P.L.83-703),1954年8月。可查阅于https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919

[4] 国家档案与记录管理局(2019)受控非机密信息(CUI)登记处。可查阅https://www.archives.gov/cui

[5] 32 CFR第2002部分(2016)，受控非机密信息(CUI),2016年9月。可查阅https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018- title32-vol6-part2002.pdf

[6] NIST(2004)安全标准联邦信息和信息系统的分类。(美国商务部，华盛顿特区)，联邦信息处理标准出版物(FIPS)199。https://doi.org/10.6028/NIST.FIPS.199

[7] NIST(2006)联邦信息和信息系统的最低安全要求。(美国商务部，华盛顿特区)，联邦信息处理标准出版物(FIPS)200。https://doi.org/10.6028/NIST.FIPS.200

[8] 联合工作组(2020)信息系统和组织的安全与隐私控制。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-53第5版，包含截至2020年12月10日的更新。https://doi.org/10.6028/NIST.SP.800-53r5

[9] 联邦信息安全现代化法案(P.L.113-283),2014年12月。可查阅https://www.govinfo.gov/app/details/PLAW-113publ28

[10] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R(2021)开发网络弹性系统：系统安全工程方法。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-160第2卷第1版。https://doi.org/10.6028/NIST.SP.800-160v2r1

[11] Ross R, Winstead M, McEvilley M(2022)工程可信安全系统。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-160第1卷第1版。https://doi.org/10.6028/NIST.SP.800-160v1r1

[12] 联合工作组(2020)系统和组织的控制基线。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-53B，包含截至2020年12月10日的更新。https://doi.org/10.6028/NIST.SP.800-53B

[13] 管理和预算办公室A-130号通告，将信息作为战略资源管理，2016年7月。可查阅https://www.whitehouse.gov/wp- content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[14] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2

[15] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[16] Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1

[17] Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1

[18] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1

[19] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[20] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[21] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-121, Rev. 2, Includes updates as of January 19, 2022. https://doi.org/10.6028/NIST.SP.800-121r2-upd1

[22] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[23] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-178. https://doi.org/10.6028/NIST.SP.800-178

[24] Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-192. https://doi.org/10.6028/NIST.SP.800-192

[14] Souppaya MP, Scarfone KA(2016)企业远程办公、远程访问和自带设备(BYOD)安全指南。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-46第2版。https://doi.org/10.6028/NIST.SP.800-46r2

[15] Barker EB(2020)密钥管理建议：第1部分--概述。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-57第1部分第5版。https://doi.org/10.6028/NIST.SP.800-57pt1r5

[16] Barker EB, Barker WC(2019)密钥管理建议：第2部分--密钥管理组织的最佳实践。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-57第2部分第1版。https://doi.org/10.6028/NIST.SP.800-57pt2r1

[17] Barker EB, Dang QH(2015)密钥管理建议，第3部分：特定应用的密钥管理指南。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-57第3部分第1版。https://doi.org/10.6028/NIST.SP.800-57pt3r1

[18] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1

[19] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[20] Souppaya MP, Scarfone KA(2016) 远程办公与自带设备(BYOD)安全用户指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-114, Rev.1. https://doi.org/10.6028/NIST.SP.800-114r1

[21] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA(2017) 蓝牙安全指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-121, Rev.2，包含截至2022年1月19日的更新。https://doi.org/10.6028/NIST.SP.800-121r2-upd1

[22] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA(2014) 基于属性的访问控制(ABAC)定义与考量指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-162，包含截至2019年8月2日的更新。https://doi.org/10.6028/NIST.SP.800-162

[23] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R(2016) 数据服务应用的基于属性的访问控制(ABAC)标准比较：可扩展访问控制标记语言(XACML)与下一代访问控制(NGAC)。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-178. https://doi.org/10.6028/NIST.SP.800-178

[24] Yaga DJ, Kuhn R, Hu VC(2017) 访问控制的验证与测试方法
urg, MD), NIST Special Publication (SP) 800-192. https://doi.org/10.6028/NIST.SP.800-192

[25] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[26] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and Automated Access Management Using Secure Shell (SSH). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966. https://doi.org/10.6028/NIST.IR.7966

[27] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[28] Howell G, Franklin JM, Sritapan V, Souppaya M, Scarfone K (2023) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 2. https://doi.org/10.6028/NIST.SP.800-124r2

[29] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[30] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97

[31] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[32] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[33] Boyens JM, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161, Rev. 1. https://doi.org/10.6028/NIST.SP.800-161r1

[34] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[35] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[36] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86

[25] Hu VC, Scarfone KA(2012) 访问控制系统评估指标指南。(NIST,Gaithersburg, MD),NIST Interagency or Internal Report(IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[26] Ylonen T, Turner P, Scarfone KA, Souppaya MP(2015) 使用Secure Shell(SSH)的交互式与自动化访问管理的安全性。(NIST,Gaithersburg, MD),NIST Interagency or Internal Report(IR) 7966. https://doi.org/10.6028/NIST.IR.7966

[27] Grassi PA, Garcia ME, Fenton JL(2017) 数字身份指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-63-3，包含截至2020年3月2日的更新。https://doi.org/10.6028/NIST.SP.800-63-3

[28] Howell G, Franklin JM, Sritapan V, Souppaya M, Scarfone K(2023) 企业移动设备安全管理指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-124, Rev.2. https://doi.org/10.6028/NIST.SP.800-124r2

[29] Scarfone KA, Mell PM(2007) 入侵检测与防御系统(IDPS)指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[30] Frankel SE, Eydt B, Owens L, Scarfone KA(2007) 建立无线稳健安全网络：IEEE 802.11i指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97

[31] Souppaya MP, Scarfone KA(2016) 远程办公与自带设备(BYOD)安全用户指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-114, Rev.1. https://doi.org/10.6028/NIST.SP.800-114r1

[32] Wilson M, Hash J(2003) 构建信息技术安全意识与培训计划。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[33] Boyens JM, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M(2022) 系统与组织的网络安全供应链风险管理实践。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-161, Rev.1. https://doi.org/10.6028/NIST.SP.800-161r1

[34] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[35] Kent K, Souppaya MP(2006) 计算机安全日志管理指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[36] Kent K, Chevalier S, Grance T, Dang H(2006) 将取证技术集成到事件响应中的指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86

[37] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1

[38] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[39] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[40] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

[41] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[42] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2

[43] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Volume 3: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3

[44] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4

[45] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3

[46] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167

[47] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[37] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1

[38] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[39] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[40] NIST(2015) SHA-3标准：基于置换的哈希与可扩展输出功能。(U.S.Department of Commerce,Washington, D.C.),Federal Information Processing Standards Publication(FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

[41] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D(2011) 面向安全的信息系统配置管理指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-128，包含截至2019年10月10日的更新。https://doi.org/10.6028/NIST.SP.800-128

[42] Dempsey KL, Eavy P, Moore G(2017) 安全控制的自动化支持评估：第2卷：硬件资产管理。(NIST,Gaithersburg, MD),NIST Interagency or Internal Report(IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2

[43] Dempsey KL, Eavy P, Goren N, Moore G(2018) 安全控制评估的自动化支持：第3卷：软件资产管理。(NIST,Gaithersburg, MD),NIST Interagency or Internal Report(IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3

[44] Quinn SD, Souppaya MP, Cook MR, Scarfone KA(2018) IT产品国家检查表计划：检查表用户与开发者指南。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-70, Rev.4. https://doi.org/10.6028/NIST.SP.800-70r4

[45] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D(2018) 安全内容自动化协议(SCAP)技术规范：SCAP Version 1.3。(NIST,Gaithersburg, MD),NIST Special Publication(SP) 800-126, Rev.3. https://doi.org/10.6028/NIST.SP.800-126r3

[46] Sedgewick A, Souppaya MP, Scarfone KA(2015) 应用程序白名单指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-167。https://doi.org/10.6028/NIST.SP.800-167

[47] Cichonski PR, Millar T, Grance T, Scarfone KA(2012) 计算机安全事件处理指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-61，第2版。https://doi.org/10.6028/NIST.SP.800-61r2

[48] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

[49] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[50] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[51] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111

[52] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[53] Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800-130

[54] Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-152. https://doi.org/10.6028/NIST.SP.800-152

[55] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[56] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4

[57] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[58] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[48] Grance T, Nolan T, Burke K, Dudley R, White G, Good T(2006) IT 计划与能力测试、培训和演练计划指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-84。https://doi.org/10.6028/NIST.SP.800-84

[49] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM(2011) 联邦信息系统和组织的信息安全持续监控(ISCM)。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-137。https://doi.org/10.6028/NIST.SP.800-137

[50] Kissel RL, Regenscheid AR, Scholl MA, Stine KM(2014) 介质净化指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-88，第1版。https://doi.org/10.6028/NIST.SP.800-88r1

[51] Scarfone KA, Souppaya MP, Sexton M(2007) 终端用户设备存储加密技术指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-111。https://doi.org/10.6028/NIST.SP.800-111

[52] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D(2010) 联邦信息系统应急计划指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-34，第1版，包含截至2010年11月11日的更新。https://doi.org/10.6028/NIST.SP.800-34r1

[53] Barker EB, Smid ME, Branstad DK, Chokhani S(2013) 设计框架
加密密钥管理系统。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-130。https://doi.org/10.6028/NIST.SP.800-130

[54] Barker EB, Branstad DK, Smid ME(2015) 美国联邦加密密钥管理系统(CKMS)概要。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-152。https://doi.org/10.6028/NIST.SP.800-152

[55] 联合任务组转型倡议(2012) 风险评估实施指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-30，第1版。https://doi.org/10.6028/NIST.SP.800-30r1

[56] Souppaya MP, Scarfone KA(2022) 企业补丁管理规划指南：技术的预防性维护。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-40，第4版。https://doi.org/10.6028/NIST.SP.800-40r4

[57] 联合任务组转型倡议(2022) 评估信息系统和组织中的安全与隐私控制。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-53A，第5版。https://doi.org/10.6028/NIST.SP.800-53Ar5

[58] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD(2008) 信息安全测试与评估技术指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-115。https://doi.org/10.6028/NIST.SP.800-115

[59] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[60] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[61] Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1. https://doi.org/10.6028/NIST.SP.800-12r1

[62] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[63] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[64] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1

[65] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B

[66] Rose S, Borchert O, Mitchell S, Connelly S (2017) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[67] Sriram K, Montgomery D (2019) Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-189. https://doi.org/10.6028/NIST.SP.800-189

[68] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 197, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

[69] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2

[70] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-177, Rev. 1. https://doi.org/10.6028/NIST.SP.800-177r1

[59] 联合任务组(2018) 信息系统和组织的风险管理框架：安全与隐私的系统生命周期方法。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-37，第2版。https://doi.org/10.6028/NIST.SP.800-37r2

[60] 联合任务组转型倡议(2011) 管理信息安全风险：组织、任务和信息系统视角。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-39。https://doi.org/10.6028/NIST.SP.800-39

[61] Nieles M, Pillitteri VY, Dempsey KL(2017) 信息安全导论。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-12，第1版。https://doi.org/10.6028/NIST.SP.800-12r1

[62] Bowen P, Hash J, Wilson M(2006) 信息安全手册：管理者指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-100，包含截至2007年3月7日的更新。https://doi.org/10.6028/NIST.SP.800-100

[63] Swanson MA, Hash J, Bowen P(2006) 联邦信息系统安全计划制定指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-18，第1版。https://doi.org/10.6028/NIST.SP.800-18r1

[64] Scarfone KA, Hoffman P(2009) 防火墙与防火墙策略指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-41，第1版。https://doi.org/10.6028/NIST.SP.800-41r1

[65] Chandramouli R(2016) 虚拟机(VM)保护的安全虚拟网络配置。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-125B。https://doi.org/10.6028/NIST.SP.800-125B

[66] Rose S, Borchert O, Mitchell S, Connelly S(2017) 零信任架构。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-207。https://doi.org/10.6028/NIST.SP.800-207

[67] Sriram K, Montgomery D(2019) 弹性域间流量交换：BGP 安全与 DDoS 缓解。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-189。https://doi.org/10.6028/NIST.SP.800-189

[68] NIST(2001) 高级加密标准(AES)。(美国商务部，华盛顿特区)，联邦信息处理标准出版物(FIPS) 197,2023年5月9日更新。https://doi.org/10.6028/NIST.FIPS.197-upd1

[69] McKay KA, Cooper DA(2019) 传输层安全(TLS)实现的选择、配置和使用指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-52，第2版。https://doi.org/10.6028/NIST.SP.800-52r2

[70] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R(2019) 可信电子邮件。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-177，第1版。https://doi.org/10.6028/NIST.SP.800-177r1

[71] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2

[72] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95

[73] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[74] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2

[75] Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Cr2

[76] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1

[77] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2

[78] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[79] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552

[80] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331

[81] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35-subchapI-sec3502

[82] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-81-2. https://doi.org/10.6028/NIST.SP.800-81-2

[83] Dempsey K, Pillitteri V, Regenscheid A (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1

[71] Jansen W, Winograd T, Scarfone KA(2008) 活动内容与移动代码指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-28，第2版。https://doi.org/10.6028/NIST.SP.800-28ver2

[72] Singhal A, Winograd T, Scarfone KA(2007) 安全 Web 服务指南。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-95。https://doi.org/10.6028/NIST.SP.800-95

[73] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R(2018) 使用离散对数密码学的成对密钥建立方案建议。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 800-56A，第3版。https://doi.org/10.6028/NIST.SP.800-56Ar3

[74] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R(2019) 使用整数分解密码学的成对密钥建立建议。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-56B, Rev.2。https://doi.org/10.6028/NIST.SP.800-56Br2

[75] Barker EB, Chen L, Davis R(2020) 密钥建立方案中的密钥派生方法建议。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-56C, Rev.2。https://doi.org/10.6028/NIST.SP.800-56Cr2

[76] Souppaya MP, Scarfone KA(2013) 台式机和笔记本电脑恶意软件事件预防与处理指南。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-83, Rev.1。https://doi.org/10.6028/NIST.SP.800-83r1

[77] Tracy MC, Jansen W, Scarfone KA, Butterfield J(2007) 电子邮件安全指南。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-45, Version 2。https://doi.org/10.6028/NIST.SP.8

[78] 国家安全系统委员会(2022) 国家安全系统委员会(CNSS)术语表。(National Security Agency，马里兰州米德堡),CNSS Instruction 4009。可访问https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[79] 《美国法典》第44编第3552条，定义。2017年版。可查阅于 https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35- 第二分章-第3552节

[80] Title 40 U.S.Code, Sec.11331，联邦信息系统标准的职责。2017 ed。可访问https://www.govinfo.gov/app/details/USCODE-2017- title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331

[81] 《美国法典》第44编第3502条，定义。2017年版。可查阅 https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35- subchapI-sec3502

[82] Chandramouli R, Rose SW(2013) 安全域名系统(DNS)部署指南。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-81-2。https://doi.org/10.6028/NIST.SP.800-81-2

[83] Dempsey K, Pillitteri V, Regenscheid A(2021) 管理信息交换的安全。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-47, Rev.1。https://doi.org/10.6028/NIST.SP.800-47r1

[84] Ross R, Pillitteri V (2024) Assessing Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-171Ar3

[84] Ross R, Pillitteri V(2024) 评估受控非机密信息的安全要求。(NIST，马里兰州盖瑟斯堡),NIST Special Publication(SP) 800-171A, Rev.3。https://doi.org/10.6028/NIST.SP.800-171Ar3

Appendix A. Acronyms

CFR
Code of Federal Regulations

CISA
Cybersecurity and Infrastructure Security Agency

CUI
Controlled Unclassified Information

CVE
Common Vulnerabilities and Exposures

CVSS
Common Vulnerability Scoring System

CWE
Common Weakness Enumeration

DMZ
Demilitarized Zone

EAP
Extensible Authentication Protocol

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

FTP
File Transfer Protocol

GMT
Greenwich Mean Time

HSM
Hardware Security Module

IEEE
Institute of Electrical and Electronics Engineers

IIoT
Industrial Internet of Things

IoT
Internet of Things

ISOO
Information Security Oversight Office

附录 A.缩略语

CFR
联邦法规

CISA
网络安全和基础设施安全局

CUI
受控非机密信息

CVE
通用漏洞与暴露

CVSS
通用漏洞评分系统

CWE
通用缺陷枚举

DMZ
非军事区

EAP
可扩展认证协议

FIPS
联邦信息处理标准

FISMA
《联邦信息安全现代化法案》

FTP
文件传输协议

GMT
格林尼治标准时间

HSM
硬件安全模块

IEEE
电气与电子工程师协会

IIoT
工业物联网

物联网
物联网

ISOO
信息安全监督办公室

IT
Information Technology

LSI
Large-Scale Integration

MAC
Media Access Control

NARA
National Archives and Records Administration

NVD
National Vulnerability Database

ODP
Organization-Defined Parameter

OT
Operational Technology

PII
Personally Identifiable Information

PIN
Personal Identification Number

PROM
Programmable Read-Only Memory

ROM
Read-Only Memory

SCAP
Security Content Automation Protocol

SCRM
Supply Chain Risk Management

TCP/IP
Transmission Control Protocol/Internet Protocol

TLS
Transport Layer Security

UTC
Coordinated Universal Time

IT
信息技术

LSI
大规模集成

MAC
媒体访问控制

NARA
国家档案与记录管理局

NVD
国家漏洞数据库

ODP
组织定义参数

OT
运营技术

PII
个人可识别信息

PIN
个人识别码

PROM
可编程只读存储器

ROM
只读存储器

SCAP
安全内容自动化协议

SCRM
供应链风险管理

TCP/IP
传输控制协议/互联网协议

TLS
传输层安全

UTC
协调世界时

Appendix B. Glossary

Appendix B provides definitions for the terminology used in SP 800-171r3. The definitions are consistent with the definitions contained in the National Information Assurance Glossary [78] unless otherwise noted.

agency
Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. [13]

assessment
See *security control assessment*.

assessor
See *security control assessor*.

audit log
A chronological record of system activities, including records of system accesses and operations performed in a given period.

audit record
An individual entry in an audit log related to an audited event.

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [7, adapted].

availability
Ensuring timely and reliable access to and use of information. [79]

advanced persistent threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives. [60]

authenticator
Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was previously referred to as a token.

baseline configuration
A documented set of specifications for a system or a configuration item within a system that has been formally reviewed and agreed upon at a given point in time, and that can only be changed through change control procedures.

common secure configuration
Recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet

附录B.术语表

附录B提供了SP 800-171r3中使用的术语定义。除非另有说明，这些定义与《国家信息保障术语表》[78]中的定义一致。

机构
任何行政机构或部门、军事部门、联邦政府公司、联邦政府控制的公司，或联邦政府行政部门中的其他机构，或任何独立监管机构。[13]

评估
见安全控制评估。

评估员
见安全控制评估员。

审计日志
系统活动的时间顺序记录，包括在给定时间段内执行的系统访问和操作的记录。

审计记录
与已审计事件相关的审计日志中的单条记录。

身份验证
验证用户、进程或设备的身份，通常作为允许访问系统中资源的先决条件。[7，改编]。

可用性
确保及时、可靠地访问和使用信息。

高级持续性威胁
具备高水平专业知识和大量资源的对手，能够利用多种攻击向量(例如网络、物理和欺骗手段)创造机会以实现其目标。这些目标通常包括在目标组织的IT基础设施中建立并扩展立足点，以窃取信息、破坏或阻碍任务、计划或组织的关键环节；或为将来实施这些目标进行布局。高级持续威胁在较长时期内反复追求其目标；适应防御者的抵抗努力；并决心维持执行其目标所需的交互水平。[60]

认证器
声明者拥有并控制的、用于验证声明者身份的事物(通常是加密模块或密码)。此前称为令牌。

基线配置
系统或系统中配置项的已记录规范集，该规范集已在特定时间点经过正式审查并达成一致，且只能通过变更控制程序进行更改。

通用安全配置
公认的、标准化的和已建立的基准，规定了特定信息技术平台/产品的安全配置设置，以及配置这些系统组件以满足

operational requirements. These benchmarks are also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides.

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [79]

configuration management
A collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

configuration settings
The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.

controlled area
Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

controlled unclassified information
Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [1]

CUI Executive Agent
The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO). [5]

CUI program
The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry. [5]

CUI registry
The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. [5]

cyber-physical systems
Interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

executive agency
An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.

external network
A network not controlled by the organization.

运行要求的说明。这些基准也称为安全配置检查表、锁定和加固指南、安全参考指南和安全技术实施指南。

保密性
维护对信息访问和披露的授权限制，包括保护个人隐私和专有信息的手段。[79]

配置管理
一组活动，侧重于通过在整个系统开发生命周期中控制这些产品和系统的初始化、变更和监控过程，来建立和维护信息技术产品和系统的完整性。

配置设置
可在硬件、软件或固件中更改的、影响系统安全态势和/或功能的参数集。

受控区域
组织确信所提供的物理和程序保护足以满足为保护信息或系统而建立的要求的任何区域或空间。

受控非机密信息
法律、法规或政府范围政策要求实施保护或传播控制的信息，不包括根据2009年12月29日第13526号行政命令《国家安全机密信息》或任何前任或继任命令，或经修订的1954年《原子能法》归类为机密的信息。[1]

CUI执行代理
国家档案和记录管理局(NARA)，负责实施行政部门范围的CUI计划，并监督联邦机构遵守第13556号行政命令的行动。NARA已将此项权力授予信息安全监督办公室(ISOO)主任。[5]

CUI 计划
行政部门范围的计划，旨在标准化所有联邦机构的CUI处理。该计划包括由第13556号行政命令、32 CFR Part 2002和CUI注册表建立的CUI规则、组织和程序。[5]

CUI 注册表
关于处理CUI的所有信息、指南、政策和要求的在线存储库，包括CUI执行代理发布的所有内容(32 CFR Part 2002除外)。除其他信息外，CUI注册表标识所有经批准的CUI类别，提供每个类别的一般描述，确定控制基础，建立标记，并包括处理程序指南。[5]

信息物理系统
通过集成物理和逻辑为功能而设计的交互式数字、模拟、物理和人力组件。

行政机构
5 U.S.C.Sec.101中规定的行政部门；5 U.S.C.Sec.102中规定的军事部门；5 U.S.C.Sec.104(1)中定义的独立机构；以及完全受31 U.S.C.Chapter 91条款约束的全资政府公司。

外部网络
不受组织控制的网络。

external service provider
See *external system service provider*.

external system (or component)
A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

external system service
A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by but not a part of the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

external system service provider
A provider of external system services to an organization through a variety of consumer-producer relationships, including joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. [8]

facility
One or more physical locations containing systems or system components that process, store, or transmit information.

federal agency
See *executive agency*.

federal information system
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [80]

FIPS-validated cryptography
A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet the requirements specified in FIPS Publication 140-3 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-approved cryptography*.

firmware
Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software*. [78]

hardware
The material physical components of a system. See *software* and *firmware*. [78]

identifier
Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

A unique label used by a system to indicate a specific entity, object, or group.

impact
With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of

外部服务提供商
参见外部系统服务提供商。

外部系统(或组件)
组织建立的授权边界之外的系统或系统组件，组织通常无法直接控制其所需安全控制的应用或安全控制有效性的评估。

外部系统服务
在组织系统授权边界之外实现的系统服务(即由组织系统使用但不属于组织系统组成部分的服务)，组织通常无法直接控制其所需安全控制措施的实施或安全控制有效性的评估。

外部系统服务提供商
通过多种消费者-生产者关系向组织提供外部系统服务的提供方，包括合资企业、商业合作伙伴关系、外包安排(即通过合同、机构间协议、业务线安排)、许可协议和/或供应链交换。[8]

设施
包含处理、存储或传输信息的系统或系统组件的一个或多个物理位置。

联邦机构
见执行机构。

联邦信息系统
由行政机构、行政机构的承包商或代表行政机构的另一组织使用或运行的信息系统。[80]

经FIPS验证的密码技术
经密码模块验证计划(CMVP)验证符合 FIPS 出版物 140-3(经修订)规定要求的密码模块。作为 CMVP 验证的前提条件，密码模块须采用已成功通过密码算法验证计划(CAVP)验证测试的密码算法实现。参见*NSA* 批准的密码术。

固件
存储在硬件中的计算机程序和数据--通常存储在只读存储器(ROM)或可编程只读存储器(PROM)中--使得这些程序和数据在程序执行期间无法被动态写入或修改。参见硬件和软件。[78]

硬件
系统的实体物理组件。参见软件和固件。[78]

标识符
用于表示个人身份及相关属性的唯一数据。姓名或卡号即为标识符的示例。

系统用来指示特定实体、对象或组的唯一标签。

影响
就安全而言，指组织运营、组织资产、个人、其他组织或国家（包括美国的国家安全利益）因丧失

confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

impact value
The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high. [6]

incident
An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [79]

information
Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [13]

information flow control
Procedure to ensure that information transfers within a system do not violate the security policy.

information resources
Information and related resources, such as personnel, equipment, funds, and information technology. [81]

information security
The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [79]

information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [81]

information technology
Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. [13]

insider threat
The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

integrity
Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [79]

信息或系统的保密性、完整性或可用性。就隐私而言，指信息系统处理个人身份信息(PII)时个人可能遭受的不利影响。

影响值
信息保密性、完整性或可用性受损可能导致的经评估的最坏情况潜在影响，以低、中或高值表示。[6]

事件
在无合法授权的情况下实际或即将危害信息或信息系统保密性、完整性或可用性的发生情况；或构成违反或即将威胁违反法律、安全策略、安全程序或可接受使用策略的情况。[79]

信息
以任何介质或形式对知识(如事实、数据或意见)的任何通信或表示，包括文本、数值、图形、制图、叙述、电子或视听形式。[13]

信息流控制
确保系统内的信息传输不违反安全策略的程序。

信息资源
信息及相关资源，如人员、设备、资金和信息技术。[81]

信息安全
保护信息和系统免遭未经授权的访问、使用、披露、中断、修改或破坏，以提供保密性、完整性和可用性。[79]

信息系统
为信息的收集、处理、维护、使用、共享、传播或处置而组织的一组离散的信息资源。[81]

信息技术
机构在数据或信息的自动获取、存储、分析、评估、处理、管理、移动、控制、显示、交换、互换、传输或接收中使用的任何服务、设备或互连系统或设备子系统。就本定义而言，此类服务或设备须由机构直接使用，或由承包商依据与机构签订的合同使用，且该合同要求使用此类服务或设备；或在履行服务或提供产品时在很大程度上使用此类服务或设备。信息技术包括计算机、辅助设备(包括安全与监视所需的成像外围设备、输入、输出和存储设备)、设计为由计算机中央处理单元控制的外围设备、软件、固件及类似程序、服务(包括云计算和帮助台服务，或支持设备或服务生命周期任一环节的其他专业服务)以及相关资源。信息技术不包括承包商附带于合同而获取且合同不要求其使用的任何设备。[13]

内部威胁
内部人员有意或无意利用其授权访问权限危害美国安全的威胁。该威胁可包括通过间谍活动、恐怖主义、未经授权的披露或通过部门资源或能力的丧失或退化对美国造成的损害。

完整性
防范信息的不当修改或破坏，并包括确保信息的不可否认性和真实性。[79]

internal network
A network in which the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors or in which the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.

least privilege
The principle that a security architecture is designed so that each entity is granted the minimum system authorizations and resources needed to perform its function.

malicious code
Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system. Examples of malicious code include viruses, worms, Trojan horses, spyware, some forms of adware, or other code-based entities that infect a host.

media
Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system. [7]

mobile code
Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

mobile device
A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable, or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and e-readers.

multi-factor authentication
Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric). See *authenticator*.

network
A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access
Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, the internet).

nonfederal organization
An entity that owns, operates, or maintains a nonfederal system.

nonfederal system
A system that does not meet the criteria for a federal system.

内部网络
安全控制的建立、维护和配置由组织员工或承包商直接控制的网络，或在组织控制的端点之间实施的密码封装或类似安全技术提供同等效果(就保密性和完整性而言)的网络。内部网络通常为组织所有，但也可能由组织控制而不为组织所有。

最小权限
安全架构的设计原则，即授予每个实体执行其功能所需的最低系统授权和资源。

恶意代码
旨在执行未经授权的进程并对系统的保密性、完整性或可用性产生不利影响的软件或固件。恶意代码的示例包括病毒、蠕虫、特洛伊木马、间谍软件、某些形式的广告软件或其他感染主机的基于代码的实体。

媒体
包括但不限于磁带、光盘、磁盘、大规模集成(LSI)存储芯片和打印输出(不包括显示媒体)在内的物理设备或书写表面，信息被记录、存储或打印在系统内的这些介质上。[7]

移动代码
从远程系统获取、通过网络传输并在本地系统上执行的软件程序或程序部分，无需接收方明确安装或执行。

移动设备
一种便携式计算设备，其外形小巧，便于单人轻松携带；设计为无需物理连接即可运行(例如，无线传输或接收信息)；具备本地、不可移除或可移除的数据存储；并包含自备电源。移动设备还可包括语音通信功能、允许设备捕获信息的板载传感器，或将本地数据与远程位置同步的内置功能。示例包括智能手机、平板电脑和电子阅读器。

多因素认证
使用两个或多个不同因素进行身份验证以实现身份验证。因素包括你知道的某些东西(例如PIN、密码)、你拥有的某些东西(例如密码识别设备、令牌)或你本身的某些特征(例如生物识别)。参见身份验证器。

网络
由一组互连组件实现的系统。此类组件可能包括路由器、集线器、布线、电信控制器、密钥分发中心和技术控制设备。

网络访问
用户(或代表用户行事的进程)通过网络(例如局域网、广域网、互联网)通信对系统的访问。

非联邦组织
拥有、运营或维护非联邦系统的实体。

非联邦系统
不符合联邦系统标准的系统。

nonlocal maintenance
Maintenance activities conducted by individuals communicating through an external network (e.g., the internet) or an internal network.

NSA-approved cryptography
Cryptography that consists of an approved algorithm, an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a specific environment, and a supporting key management infrastructure. [8]

on behalf of (an agency)
A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government. [5]

organization
An entity of any size, complexity, or positioning within an organizational structure. [7, adapted]

organization-defined parameter
The variable part of a security requirement that is instantiated by an organization during the tailoring process by assigning an organization-defined value as part of the requirement. [8, adapted]

overlay
A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. [13]

personnel security
The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness. [8]

portable storage device
A system component that can be inserted into and removed from a system and that is used to store information or data (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., compact/digital video disks, flash/thumb drives, external solid-state drives, external hard disk drives, flash memory cards/drives that contain nonvolatile memory).

potential impact
The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals. [6]

privileged account
A system account with the authorizations of a privileged user.

privileged user
A user who is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

records
The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results) that serve as a basis for verifying that the organization and the system are performing as

非本地维护
由通过外部网络(例如互联网)或内部网络通信的个人进行的维护活动。

NSA批准的密码技术
由经批准的算法、已在特定环境中获准用于保护机密信息和/或受控非机密信息的实现以及支持性密钥管理基础设施组成的密码学。[8]

代表(某机构)
在以下情况下出现的情形：(i) 非行政部门实体使用或操作信息系统，或维护或收集信息以处理、存储或传输联邦信息；且(ii) 这些活动并非附带于向政府提供服务或产品。[5]

组织
在组织结构中具有任何规模、复杂性或定位的实体。[7，改编]

组织定义的参数
安全要求中的可变部分，由组织在裁剪过程中通过指定组织定义值作为要求的一部分来实例化。[8，改编]

覆盖层
在裁剪过程中使用的安全或隐私控制、控制增强、补充指南及其他支持信息的规范，旨在补充(并进一步完善)安全控制基线。覆盖层规范可能比原始安全控制基线规范更严格或更宽松，并可应用于多个信息系统。[13]

人员安全
评估个人在需要可信性的职责和责任方面的行为、诚信、判断力、忠诚度、可靠性和稳定性的学科。[8]

便携式存储设备
可插入系统并从系统中移除的系统组件，用于存储信息或数据(例如文本、视频、音频和/或图像数据)。此类组件通常实现在磁、光或固态设备上(例如压缩/数字视频光盘、闪存/拇指驱动器、外部固态驱动器、外部硬盘驱动器、包含非易失性存储器的闪存卡/驱动器)。

潜在影响
保密性、完整性或可用性的丧失可预期对组织运营、组织资产或个人产生：(i) 有限的不利影响(FIPS Publication 199低)；(ii) 严重的不利影响(FIPS Publication 199中)；或(iii) 严重或灾难性的不利影响(FIPS Publication 199高)。[6]

特权账户
具有特权用户授权的系统账户。

特权用户
被授权(因此被信任)执行普通用户无权执行的安全相关功能的用户。

记录
已执行活动或已取得结果的证据记录(自动和/或手动)(例如表单、报告、测试结果)，用作验证组织和系统按

intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain a complete set of information on particular items).

remote access
Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the internet). Remote access methods include dial-up, broadband, and wireless.

remote maintenance
Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).

replay resistance
Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [13]

risk assessment
The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. [55]

sanitization
Actions taken to render data written on media unrecoverable by ordinary and — for some forms of sanitization — extraordinary means.

A process to remove information from media such that data recovery is not possible, including the removal of all classified labels, markings, and activity logs.

security
A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. [78]

security assessment
See *security control assessment*.

security control
The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [13]

security control assessment
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [13]

security domain
A domain that implements a security policy and is administered by a single authority. [78, adapted]

预期运行的依据。也用于指相关数据字段的单元(即可由程序访问并包含特定项目完整信息集的数据字段组)。

远程访问
用户(或代表用户行事的进程)通过外部网络(例如互联网)通信对组织系统的访问。远程访问方法包括拨号、宽带和无线。

远程维护
由通过外部网络(例如互联网)通信的个人进行的维护活动。

重放抵抗
防止截获传输中的身份验证或访问控制信息及其后续重传以产生未经授权效果或获得未经授权访问的保护。

风险
实体受潜在情况或事件威胁程度的度量，通常是以下因素的函数：(i) 如果该情况或事件发生将产生的不利影响或损害程度；以及(ii) 发生的可能性。[13]

风险评估
识别因系统运行而对组织运营(包括任务、功能、形象、声誉)、组织资产、个人、其他组织和国家产生的风险的过程。

[55]

清除
为使写入介质的数据无法通过普通手段--对于某些形式的净化而言，还包括非常规手段--恢复而采取的操作。

从介质中移除信息以使数据恢复成为不可能的过程，包括移除所有密级标签、标记和活动日志。

安全
因建立并维持保护措施而产生的一种状态，这些保护措施使组织能够在其系统使用面临威胁所带来风险的情况下仍执行其任务或关键功能。保护措施可能涉及威慑、规避、预防、检测、恢复和纠正的组合，应构成组织风险管理方法的一部分。[78]

安全评估
见安全控制评估。

安全控制
为信息系统或组织规定的、用以保护系统及其信息的保密性、完整性和可用性的保障措施或对策。[13]

安全控制评估
对安全控制进行的测试或评估，以确定控制被正确实施、按预期运行并在满足信息系统或组织安全要求方面产生预期结果的程度。[13]

安全域
实施安全策略并由单一权威机构管理的域。[78，改编]

security functions
The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

security requirement
A requirement levied on a system or an organization that is derived from applicable laws, Executive Orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. [7, adapted] [8, adapted]

system
See *information system*.

system component
A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware. [41]

system security plan
A document that describes how an organization meets or plans to meet the security requirements for a system. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are satisfied, and the relationships with or connections to other systems.

system service
A capability provided by a system that facilitates information processing, storage, or transmission.

threat
Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [55]

system user
An individual or (system) process acting on behalf of an individual that is authorized to access a system.

安全功能
系统中负责执行系统安全策略并支持代码和数据隔离(保护所依据的隔离)的硬件、软件或固件。

安全要求
对系统或组织提出的要求，源自适用的法律、行政命令、指令、法规、政策、标准、程序或任务/业务需要，以确保正在处理、存储或传输的信息的保密性、完整性和可用性。[7，改编][8，改编]

系统
见信息系统。

系统组件
代表系统构建块的离散可识别信息技术资产，可能包括硬件、软件和固件。[41]

系统安全计划
描述组织如何满足或计划满足系统安全要求的文档。特别是，系统安全计划描述系统边界、系统运行的环境、如何满足安全要求以及与其他系统的关系或连接。

系统服务
由系统提供的、促进信息处理、存储或传输的能力。

威胁
通过系统经由未授权访问、破坏、泄露、信息修改和/或拒绝服务，可能对组织运营、组织资产、个人、其他组织或国家产生不利影响的任何情况或事件。[55]

系统用户
代表个人行事且被授权访问系统的个人或(系统)进程。

Appendix C. Tailoring Criteria

This appendix describes the security control tailoring criteria used to develop the CUI security requirements. Table 2 lists the available tailoring options and the shorthand tailoring symbols. Table 3 through Table 22 specify the tailoring actions applied to the controls in the SP 800-53 moderate baseline [12] to obtain the security requirements in Sec. 3. The controls and control enhancements are hyperlinked to the NIST Cybersecurity and Privacy Reference Tool, which provides online access to the specific control language and supplemental materials in SP 800-53.

Table 2. Security Control Tailoring Criteria

TAILORING SYMBOL	TAILORING CRITERIA
NCO	The control is not directly related to protecting the confidentiality of CUI.
FED	The control is primarily the responsibility of the Federal Government.
ORC	The outcome of the control related to protecting the confidentiality of CUI is adequately covered by other related controls.[16]
N/A	The control is not applicable.
CUI	The control is directly related to protecting the confidentiality of CUI.

Table 3. Access Control (AC)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AC-01	Policy and Procedures	CUI	03.15.01
AC-02	Account Management	CUI	03.01.01
AC-02(01)	Account Management | Automated System Account Management	NCO	—
AC-02(02)	Account Management | Automated Temporary and Emergency Account Management	NCO	—
AC-02(03)	Account Management | Disable Accounts	CUI	03.01.01
AC-02(04)	Account Management | Automated Audit Actions	NCO	—
AC-02(05)	Account Management | Inactivity Logout	CUI	03.01.01
AC-02(13)	Account Management | Disable Accounts for High-Risk Individuals	CUI	03.01.01
AC-03	Access Enforcement	CUI	03.01.02
AC-04	Information Flow Enforcement	CUI	03.01.03
AC-05	Separation of Duties	CUI	03.01.04
AC-06	Least Privilege	CUI	03.01.05
AC-06(01)	Least Privilege | Authorize Access to Security Functions	CUI	03.01.05

[16] The security controls in SP 800-53 provide a comprehensive set of security capabilities needed to protect organizational systems and support the concept of defense in depth. Some of the security controls may address similar or overlapping security topics that are covered by other related controls. These controls have been designated as ORC in the tailoring criteria.

附录 C.裁剪准则

本附录描述了用于制定CUI安全要求的安全控制裁剪准则。表2列出了可用的裁剪选项和简写裁剪符号。表3至表22规定了为获得第3节中的安全要求而对SP 800-53中等基线[12]中的控制所应用的裁剪操作。这些控制和控制增强项已超链接至NIST网络安全与隐私参考工具，该工具提供对SP 800-中具体控制语言和补充材料的在线访问。

53.

表 2. 安全控制裁剪准则

裁剪符号	裁剪标准
NCO	该控制措施与保护CUI的机密性没有直接关系。
FED	该控制措施主要由联邦政府负责。
ORC	与保护 CUI 保密性相关的控制结果是否充分由其他相关控制项覆盖。[16]
不适用	该控制项不适用。
CUI	该控制措施直接关系到保护CUI的机密性。

表 3. 访问控制(AC)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
AC-01	策略与程序	CUI	03.15.01
AC-02	账户管理	CUI	03.01.01
AC-02(01)	账户管理 | 自动化系统账户管理	NCO	-
AC-02(02)	账户管理 | 自动化临时和紧急账户管理	NCO	-
AC-02(03)	账户管理 | 禁用账户	CUI	03.01.01
AC-02(04)	账户管理 | 自动化审计操作	NCO	-
AC-02(05)	账户管理 | 不活动注销	CUI	03.01.01
AC-02(13)	账户管理 | 对高风险账户禁用个人	CUI	03.01.01
AC-03	访问强制	CUI	03.01.02
AC-04	信息流强制	CUI	03.01.03
AC-05	职责分离	CUI	03.01.04
AC-06	最小权限	CUI	03.01.05
AC-06(01)	最小权限 | 授权访问安全功能	CUI	03.01.05

[16] SP 800-53 中的安全控制提供了一套全面的安全能力，用于保护组织系统并支持纵深防御概念。部分安全控制可能涉及与其他相关控制所涵盖的相似或重叠的安全主题。这些控制在裁剪准则中被指定为 ORC。

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AC-06(02)	Least Privilege | Non-Privileged Access for Non-Security Functions	CUI	03.01.06
AC-06(05)	Least Privilege | Privileged Accounts	CUI	03.01.06
AC-06(07)	Least Privilege | Review of User Privileges	CUI	03.01.05
AC-06(09)	Least Privilege | Log Use of Privileged Functions	CUI	03.01.07
AC-06(10)	Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	CUI	03.01.07
AC-07	Unsuccessful Logon Attempts	CUI	03.01.08
AC-08	System Use Notification	CUI	03.01.09
AC-11	Device Lock	CUI	03.01.10
AC-11(01)	Device Lock | Pattern-Hiding Displays	CUI	03.01.10
AC-12	Session Termination	CUI	03.01.11
AC-14	Permitted Actions Without Identification or Authentication	FED	—
AC-17	Remote Access	CUI	03.01.02
AC-17(01)	Remote Access | Monitoring and Control	NCO	—
AC-17(02)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	CUI	03.13.08
AC-17(03)	Remote Access | Managed Access Control Points	CUI	03.01.12
AC-17(04)	Remote Access | Privileged Commands and Access	CUI	03.01.12
AC-18	Wireless Access	CUI	03.01.16
AC-18(01)	Wireless Access | Authentication and Encryption	CUI	03.01.16
AC-18(03)	Wireless Access | Disable Wireless Networking	CUI	03.01.16
AC-19	Access Control for Mobile Devices	CUI	03.01.18
AC-19(05)	Access Control for Mobile Devices | Full Device or Container-Based Encryption	CUI	03.01.18
AC-20	Use of External Systems	CUI	03.01.20
AC-20(01)	Use of External Systems | Limits on Authorized Use	CUI	03.01.20
AC-20(02)	Use of External Systems | Portable Storage Devices – Restricted Use	CUI	03.01.20
AC-21	Information Sharing	FED	—
AC-22	Publicly Accessible Content	CUI	03.01.22

Table 4. Awareness and Training (AT)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AT-01	Policy and Procedures	CUI	03.15.01
AT-02	Literacy Training and Awareness	CUI	03.02.01
AT-02(02)	Literacy Training and Awareness | Insider Threat	CUI	03.02.01
AT-02(03)	Literacy Training and Awareness | Social Engineering and Mining	CUI	03.02.01
AT-03	Role-Based Training	CUI	03.02.02

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
AC-06(02)	最小权限 | 非安全功能非特权访问 | 功能	CUI	03.01.06
AC-06(05)	最小权限 | 特权账户	CUI	03.01.06
AC-06(07)	最小权限 | 用户权限审查	CUI	03.01.05
AC-06(09)	最小权限 | 记录特权功能的使用	CUI	03.01.07
AC-06(10)	最小权限 | 禁止非特权用户执行特权功能	CUI	03.01.07
AC-07	不成功登录尝试	CUI	03.01.08
AC-08	系统使用通知	CUI	03.01.09
AC-11	设备锁定	CUI	03.01.10
AC-11(01)	设备锁定 | 图案隐藏显示	CUI	03.01.10
AC-12	会话终止	CUI	03.01.11
AC-14	允许在未识别或未认证情况下执行的操作	FED	-
AC-17	远程访问	CUI	03.01.02
AC-17(01)	远程访问 | 监控与控制	NCO	-
AC-17(02)	远程访问 | 使用加密保护保密性和完整性 | 加密	CUI	03.13.08
AC-17(03)	远程访问 | 受管访问控制点	CUI	03.01.12
AC-17(04)	远程访问 | 特权命令与访问	CUI	03.01.12
AC-18	无线访问	CUI	03.01.16
AC-18(01)	无线访问 | 认证与加密	CUI	03.01.16
AC-18(03)	无线访问 | 禁用无线网络	CUI	03.01.16
AC-19	移动设备的访问控制	CUI	03.01.18
AC-19(05)	移动设备的访问控制 | 全设备或容器 | 基于加密	CUI	03.01.18
AC-20	外部系统的使用	CUI	03.01.20
AC-20(01)	外部系统的使用 | 授权使用的限制	CUI	03.01.20
AC-20(02)	外部系统的使用 | 便携式存储设备 - 受限使用	CUI	03.01.20
AC-21	信息共享	FED	-
AC-22	公开可访问内容	CUI	03.01.22

表 4. 意识和培训(AT)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
AT-01	策略和程序	CUI	03.15.01
AT-02	素养培训与意识	CUI	03.02.01
AT-02(02)	素养培训与意识 | 内部威胁	CUI	03.02.01
AT-02(03)	素养培训与意识 | 社会工程与挖掘 CUI 03.02.01		
AT-03	基于角色的培训	CUI	03.02.02

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AT-04	Training Records	NCO	—

Table 5. Audit and Accountability (AU)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
AU-01	Policy and Procedures	CUI	03.15.01
AU-02	Event Logging	CUI	03.03.01
AU-03	Content of Audit Records	CUI	03.03.02
AU-03(01)	Additional Audit Information	CUI	03.03.02
AU-04	Audit Log Storage Capacity	NCO	—
AU-05	Response to Audit Logging Process Failures	CUI	03.03.04
AU-06	Audit Record Review, Analysis, and Reporting	CUI	03.03.05
AU-06(01)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	NCO	—
AU-06(03)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	CUI	03.03.05
AU-07	Audit Record Reduction and Report Generation	CUI	03.03.06
AU-07(01)	Audit Record Reduction and Report Generation | Automatic Processing	NCO	—
AU-08	Time Stamps	CUI	03.03.07
AU-09	Protection of Audit Information	CUI	03.03.08
AU-09(04)	Protection of Audit Information | Access by Subset of Privileged Users	CUI	03.03.08
AU-11	Audit Record Retention	CUI	03.03.03
AU-12	Audit Record Generation	CUI	03.03.03

Table 6. Assessment, Authorization, and Monitoring (CA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CA-01	Policy and Procedures	CUI	03.15.01
CA-02	Control Assessments	CUI	03.12.01
CA-02(01)	Control Assessments | Independent Assessors	NCO	—
CA-03	Information Exchange	CUI	03.12.05
CA-05	Plan of Action and Milestones	CUI	03.12.02
CA-06	Authorization	FED	—
CA-07	Continuous Monitoring	CUI	03.12.03
CA-07(01)	Continuous Monitoring | Independent Assessment	NCO	—
CA-07(04)	Continuous Monitoring | Risk Monitoring	NCO	—
CA-09	Internal System Connections	NCO	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
AT-04	培训记录	NCO	-

表 5. 审计和问责(AU)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
AU-01	策略与程序	CUI	03.15.01
AU-02	事件日志记录	CUI	03.03.01
AU-03	审计记录内容	CUI	03.03.02
AU-03(01)	附加审计信息	CUI	03.03.02
AU-04	审计日志存储容量	NCO	-
AU-05	对审计日志记录过程故障的响应	CUI	03.03.04
AU-06	审计记录审查、分析与报告	CUI	03.03.05
AU-06(01)	审计记录审查、分析与报告 | 自动化流程整合	NCO	-
AU-06(03)	审计记录审查、分析与报告 | 关联审计记录存储库	CUI	03.03.05
AU-07	审计记录缩减与报告生成	CUI	03.03.06
AU-07(01)	审计记录缩减与报告生成 | 自动处理	NCO	-
AU-08	时间戳	CUI	03.03.07
AU-09	审计信息保护	CUI	03.03.08
AU-09(04)	审计信息保护 | 特权子集访问用户	CUI	03.03.08
AU-11	审计记录保留	CUI	03.03.03
AU-12	审计记录生成	CUI	03.03.03

表 6. 评估、授权、和监控(CA)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
CA-01	策略与程序	CUI	03.15.01
CA-02	控制评估	CUI	03.12.01
CA-02(01)	控制评估 | 独立评估员	NCO	-
CA-03	信息交换	CUI	03.12.05
CA-05	行动计划与里程碑	CUI	03.12.02
CA-06	授权	FED	-
CA-07	持续监控	CUI	03.12.03
CA-07(01)	持续监控 | 独立评估	NCO	-
CA-07(04)	持续监控 | 风险监控	NCO	-
CA-09	内部系统连接	NCO	-

Table 7. Configuration Management (CM)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CM-01	Policy and Procedures	CUI	03.15.01
CM-02	Baseline Configuration	CUI	03.04.01
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency	NCO	—
CM-02(03)	Baseline Configuration | Retention of Previous Configurations	NCO	—
CM-02(07)	Baseline Configuration | Configure Systems and Components for High-Risk Areas	CUI	03.04.12
CM-03	Configuration Change Control	CUI	03.04.03
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	NCO	—
CM-03(04)	Configuration Change Control | Security and Privacy Representatives	NCO	—
CM-04	Impact Analyses	CUI	03.04.04
CM-04(02)	Impact Analyses | Verification of Controls	CUI	03.04.04
CM-05	Access Restrictions for Change	CUI	03.04.05
CM-06	Configuration Settings	CUI	03.04.02
CM-07	Least Functionality	CUI	03.04.06
CM-07(01)	Least Functionality | Periodic Review	CUI	03.04.06
CM-07(02)	Least Functionality | Prevent Program Execution	ORC	—
CM-07(05)	Least Functionality | Authorized Software – Allow by Exception	CUI	03.04.08
CM-08	System Component Inventory	CUI	03.04.10
CM-08(01)	System Component Inventory | Updates During Installation and Removal	CUI	03.04.10
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	NCO	—
CM-09	Configuration Management Plan	NCO	—
CM-10	Software Usage Restrictions	NCO	—
CM-11	User-Installed Software	ORC	—
CM-12	Information Location	CUI	03.04.11
CM-12(01)	Information Location | Automated Tools to Support Information Location	NCO	—

Table 8. Contingency Planning (CP)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CP-01	Policy and Procedures	NCO	—
CP-02	Contingency Plan	NCO	—
CP-02(01)	Contingency Plan | Coordinate With Related Plans	NCO	—
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	NCO	—

表 7. 配置管理(CM)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
CM-01	策略与程序	CUI 03.15.01	
CM-02	基线配置	CUI 03.04.01	
CM-02(02)	基线配置 | 准确性的自动化支持与货币	NCO	-
CM-02(03)	基线配置 | 先前配置的保留	NCO	-
CM-02(07)	基线配置 | 配置系统和组件用于高风险领域	CUI 03.04.12	
CM-03	配置变更控制	CUI 03.04.03	
CM-03(02)	配置变更控制 | 测试、验证与变更记录	NCO	-
CM-03(04)	配置变更控制 | 安全与隐私代表	NCO	-
CM-04	影响分析	CUI 03.04.04	
CM-04(02)	影响分析 | 控制措施验证	CUI 03.04.04	
CM-05	变更的访问限制	CUI 03.04.05	
CM-06	配置设置	CUI 03.04.02	
CM-07	最小功能	CUI 03.04.06	
CM-07(01)	最小功能 | 定期审查	CUI 03.04.06	
CM-07(02)	最小功能 | 阻止程序执行	ORC	-
CM-07(05)	最小功能 | 授权软件 - 例外允许 CUI 03.04.08		
CM-08	系统组件清单	CUI 03.04.10	
CM-08(01)	系统组件清单 | 安装期间更新及移除	CUI 03.04.10	
CM-08(03)	系统组件清单 | 自动化未授权组件检测	NCO	-
CM-09	配置管理计划	NCO	-
CM-10	软件使用限制	NCO	-
CM-11	用户安装的软件	ORC	-
CM-12	信息位置	CUI 03.04.11	
CM-12(01)	信息位置 | 支持自动化的工具信息位置	NCO	-

表 8. 应急规划(CP)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
CP-01	策略与程序	NCO	-
CP-02	应急计划	NCO	-
CP-02(01)	应急计划 | 与相关计划协调	NCO	-
CP-02(03)	应急计划 | 恢复任务和业务功能	NCO	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
CP-02(08)	Contingency Plan | Identify Critical Assets	NCO	—
CP-03	Contingency Training	NCO	—
CP-04	Contingency Plan Testing	NCO	—
CP-04(01)	Contingency Plan Testing | Coordinate Related Plans	NCO	—
CP-06	Alternate Storage Site	NCO	—
CP-06(01)	Alternate Storage Site | Separation of Primary Site	NCO	—
CP-06(03)	Alternate Storage Site | Accessibility	NCO	—
CP-07	Alternate Processing Site	NCO	—
CP-07(01)	Alternate Processing Site | Separation of Primary Site	NCO	—
CP-07(02)	Alternate Processing Site | Accessibility	NCO	—
CP-07(03)	Alternate Processing Site | Priority of Service	NCO	—
CP-08	Telecommunications Services	NCO	—
CP-08(01)	Telecommunications Services | Priority of Service Provisions	NCO	—
CP-08(02)	Telecommunications Services | Single Points of Failure	NCO	—
CP-09	System Backup	CUI	03.08.09
CP-09(01)	System Backup | Testing for Reliability and Integrity	NCO	—
CP-09(08)	System Backup | Cryptographic Protection	CUI	03.08.09
CP-10	System Recovery and Reconstitution	NCO	—
CP-10(02)	System Recovery and Reconstitution | Transaction Recovery	NCO	—

Table 9. Identification and Authentication (IA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IA-01	Policy and Procedures	CUI	03.15.01
IA-02	Identification and Authentication (Organizational Users)	CUI	03.05.01
IA-02(01)	Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts	CUI	03.05.03
IA-02(02)	Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts	CUI	03.05.03
IA-02(08)	Identification and Authentication (Organizational Users) | Access to Accounts – Replay Resistant	CUI	03.05.04
IA-02(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	FED	—
IA-03	Device Identification and Authentication	CUI	03.05.02
IA-04	Identifier Management	CUI	03.05.05
IA-04(04)	Identifier Management | Identify User Status	CUI	03.05.05
IA-05	Authenticator Management	CUI	03.05.12
IA-05(01)	Authenticator Management | Password-Based Authentication	CUI	03.05.07
IA-05(02)	Authenticator Management | Public Key-Based Authentication	FED	—
IA-05(06)	Authenticator Management | Protection of Authenticators	FED	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
CP-02(08)	应急计划 | 识别关键资产	NCO	-
CP-03	应急培训	NCO	-
CP-04	应急计划测试	NCO	-
CP-04(01)	应急计划测试 | 协调相关计划	NCO	-
CP-06	备用存储站点	NCO	-
CP-06(01)	备用存储站点 | 主站点分离	NCO	-
CP-06(03)	备用存储站点 | 可访问性	NCO	-
CP-07	备用处理站点	NCO	-
CP-07(01)	备用处理站点 | 主站点分离	NCO	-
CP-07(02)	备用处理站点 | 可访问性	NCO	-
CP-07(03)	备用处理站点 | 服务优先级	NCO	-
CP-08	电信服务	NCO	-
CP-08(01)	电信服务 | 服务优先条款	NCO	-
CP-08(02)	电信服务 | 单点故障	NCO	-
CP-09	系统备份	CUI	03.08.09
CP-09(01)	系统备份 | 可靠性与完整性测试	NCO	-
CP-09(08)	系统备份 | 加密保护	CUI	03.08.09
CP-10	系统恢复与重建	NCO	-
CP-10(02)	系统恢复与重建 | 事务恢复	NCO	-

表 9. 标识和身份验证(IA)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
IA-01	策略与程序	CUI	03.15.01
IA-02	标识与认证(组织用户)	CUI	03.05.01
IA-02(01)	识别与认证(组织用户)| 多因素对特权账户进行多因素认证	CUI	03.05.03
IA-02(02)	识别与认证(组织用户)| 多因素对非特权账户进行多因素认证	CUI	03.05.03
IA-02(08)	识别与认证(组织用户) | 访问至账户 - 防重放	CUI	03.05.04
IA-02(12)	识别与认证(组织用户) | 接受PIV凭证	FED	-
IA-03	设备标识与身份验证	CUI	03.05.02
IA-04	标识符管理	CUI	03.05.05
IA-04(04)	标识符管理 | 识别用户状态	CUI	03.05.05
IA-05	认证器管理	CUI	03.05.12
IA-05(01)	身份验证器管理 | 基于密码的身份验证	CUI	03.05.07
IA-05(02)	身份验证器管理 | 基于公钥的身份验证	FED	-
IA-05(06)	身份验证器管理 | 身份验证器保护	FED	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IA-06	Authentication Feedback	CUI	03.05.11
IA-07	Cryptographic Module Authentication	FED	—
IA-08	Identification and Authentication (Non-Organizational Users)	FED	—
IA-08(01)	Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials From Other Agencies	FED	—
IA-08(02)	Identification and Authentication (Non-Organizational Users) | Acceptance of External Authenticators	FED	—
IA-08(04)	Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles	FED	—
IA-11	Re-Authentication	CUI	03.05.01
IA-12	Identity Proofing	FED	—
IA-12(02)	Identity Proofing | Identity Evidence	FED	—
IA-12(03)	Identity Proofing | Identity Evidence Validation and Verification	FED	—
IA-12(05)	Identity Proofing | Address Confirmation	FED	—

Table 10. Incident Response (IR)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
IR-01	Policy and Procedures	CUI	03.15.01
IR-02	Incident Response Training	CUI	03.06.04
IR-03	Incident Response Testing	CUI	03.06.03
IR-03(02)	Incident Response Testing | Coordinate With Related Plans	NCO	—
IR-04	Incident Handling	CUI	03.06.01
IR-04(01)	Incident Handling | Automated Incident Handling Processes	NCO	—
IR-05	Incident Monitoring	CUI	03.06.02
IR-06	Incident Reporting	CUI	03.06.02
IR-06(01)	Incident Reporting | Automated Reporting	NCO	—
IR-06(03)	Incident Reporting | Supply Chain Coordination	NCO	—
IR-07	Incident Response Assistance	CUI	03.06.02
IR-07(01)	Incident Response Assistance | Automation Support for Availability of Information and Support	NCO	—
IR-08	Incident Response Plan	CUI	03.06.05

Table 11. Maintenance (MA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MA-01	System Maintenance Policy and Procedures	CUI	03.15.01
MA-02	Controlled Maintenance	NCO	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
IA-06	认证反馈	CUI	03.05.11
IA-07	密码模块认证	FED	-
IA-08	标识与认证(非组织用户)	FED	-
IA-08(01)	标识和身份验证(非组织用户) | 接受其他机构的PIV凭证	FED	-
IA-08(02)	标识和身份验证(非组织用户) | 接受外部认证器	FED	-
IA-08(04)	标识和身份验证(非组织用户) | 使用已定义配置文件	FED	-
IA-11	重新认证	CUI	03.05.01
IA-12	身份证明	FED	-
IA-12(02)	身份证明 | 身份证据	FED	-
IA-12(03)	身份证明 | 身份证据验证和核实	FED	-
IA-12(05)	身份验证 | 地址确认	FED	-

表 10. 事件响应(IR)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
IR-01	策略与程序	CUI	03.15.01
IR-02	事件响应培训	CUI	03.06.04
IR-03	事件响应测试	CUI	03.06.03
IR-03(02)	事件响应测试 | 与相关计划协调	NCO	-
IR-04	事件处理	CUI	03.06.01
IR-04(01)	事件处理 | 自动化事件处理流程	NCO	-
IR-05	事件监控	CUI	03.06.02
IR-06	事件报告	CUI	03.06.02
IR-06(01)	事件报告 | 自动报告	NCO	-
IR-06(03)	事件报告 | 供应链协调	NCO	-
IR-07	事件响应协助	CUI	03.06.02
IR-07(01)	事件响应协助 | 自动化支持信息与支持的可用性	NCO	-
IR-08	事件响应计划	CUI	03.06.05

表 11. 维护(MA)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
MA-01	系统维护策略和程序	CUI	03.15.01
MA-02	受控维护	NCO	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MA-03	Maintenance Tools	CUI	03.07.04
MA-03(01)	Maintenance Tools | Inspect Tools	CUI	03.07.04
MA-03(02)	Maintenance Tools | Inspect Media	CUI	03.07.04
MA-03(03)	Maintenance Tools | Prevent Unauthorized Removal	CUI	03.07.04
MA-04	Nonlocal Maintenance	CUI	03.07.05
MA-05	Maintenance Personnel	CUI	03.07.06
MA-06	Timely Maintenance	NCO	—

Table 12. Media Protection (MP)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
MP-01	Policy and Procedures	CUI	03.15.01
MP-02	Media Access	CUI	03.08.02
MP-03	Media Marking	CUI	03.08.04
MP-04	Media Storage	CUI	03.08.01
MP-05	Media Transport	CUI	03.08.05
MP-06	Media Sanitization	CUI	03.08.03
MP-07	Media Use	CUI	03.08.07

Table 13. Physical and Environmental Protection (PE)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PE-01	Policy and Procedures	CUI	03.15.01
PE-02	Physical Access Authorizations	CUI	03.10.01
PE-03	Physical Access Control	CUI	03.10.07
PE-04	Access Control for Transmission	CUI	03.10.08
PE-05	Access Control for Output Devices	CUI	03.10.07
PE-06	Monitoring Physical Access	CUI	03.10.02
PE-06(01)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	NCO	—
PE-08	Visitor Access Records	NCO	—
PE-09	Power Equipment and Cabling	NCO	—
PE-10	Emergency Shutoff	NCO	—
PE-11	Emergency Power	NCO	—
PE-12	Emergency Lighting	NCO	—
PE-13	Fire Protection	NCO	—
PE-13(01)	Fire Protection | Detection Systems – Automatic Activation and Notification	NCO	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
MA-03	维护工具	CUI	03.07.04
MA-03(01)	维护工具 | 检查工具	CUI	03.07.04
MA-03(02)	维护工具 | 检查介质	CUI	03.07.04
MA-03(03)	维护工具 | 防止未经授权的移除	CUI	03.07.04
MA-04	非本地维护	CUI	03.07.05
MA-05	维护人员	CUI	03.07.06
MA-06	及时维护	NCO	-

表 12. 介质保护(MP)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
MP-01	策略与程序	CUI	03.15.01
MP-02	介质访问	CUI	03.08.02
MP-03	介质标记	CUI	03.08.04
MP-04	媒体存储	CUI	03.08.01
MP-05	媒体传输	CUI	03.08.05
MP-06	媒体净化	CUI	03.08.03
MP-07	媒体使用	CUI	03.08.07

表 13. 物理和环境保护(PE)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PE-01	策略与程序	CUI	03.15.01
PE-02	物理访问授权	CUI	03.10.01
PE-03	物理访问控制	CUI	03.10.07
PE-04	传输访问控制	CUI	03.10.08
PE-05	输出设备的访问控制	CUI	03.10.07
PE-06	监控物理访问	CUI	03.10.02
PE-06(01)	监控物理访问 | 入侵报警与监视设备	NCO	-
PE-08	访客访问记录	NCO	-
PE-09	电力设备与布线	NCO	-
PE-10	紧急关断	NCO	-
PE-11	应急电源	NCO	-
PE-12	应急照明	NCO	-
PE-13	消防	NCO	-
PE-13(01)	消防 | 探测系统 - 自动激活与通知	NCO	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PE-14	Environmental Controls	NCO	—
PE-15	Water Damage Protection	NCO	—
PE-16	Delivery and Removal	NCO	—
PE-17	Alternate Work Site	CUI	03.10.06

Table 14. Planning (PL)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PL-01	Policy and Procedures	CUI	03.15.01
PL-02	System Security and Privacy Plans	CUI	03.15.02
PL-04	Rules of Behavior	CUI	03.15.03
PL-04(01)	Rules of Behavior | Social Media and External Site/Application Usage Restrictions	NCO	—
PL-08	Security and Privacy Architectures	NCO	—
PL-10	Baseline Selection	FED	—
PL-11	Baseline Tailoring	FED	—

Table 15. Program Management (PM)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PM-01	Information Security Program Plan	N/A	—
PM-02	Information Security Program Leadership Role	N/A	—
PM-03	Information Security and Privacy Resources	N/A	—
PM-04	Plan of Action and Milestones Process	N/A	—
PM-05	System Inventory	N/A	—
PM-05(01)	System Inventory | Inventory of Personally Identifiable Information	N/A	—
PM-06	Measures of Performance	N/A	—
PM-07	Enterprise Architecture	N/A	—
PM-07(01)	Enterprise Architecture | Offloading	N/A	—
PM-08	Critical Infrastructure Plan	N/A	—
PM-09	Risk Management Strategy	N/A	—
PM-10	Authorization Process	N/A	—
PM-11	Mission and Business Process Definition	N/A	—
PM-12	Insider Threat Program	N/A	—
PM-13	Security and Privacy Workforce	N/A	—
PM-14	Testing, Training, and Monitoring	N/A	—
PM-15	Security and Privacy Groups and Associations	N/A	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PE-14	环境控制	NCO	-
PE-15	水损防护	NCO	-
PE-16	交付与移除	NCO	-
PE-17	备用工作场所	CUI	03.10.06

表 14. 规划(PL)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PL-01	策略与程序	CUI	03.15.01
PL-02	系统安全与隐私计划	CUI	03.15.02
PL-04	行为规则	CUI	03.15.03
PL-04(01)	行为规则 | 社交媒体与外部站点/应用程序使用限制	NCO	-
PL-08	安全与隐私架构	NCO	-
PL-10	基线选择	FED	-
PL-11	基线裁剪	FED	-

表 15. 计划管理(PM)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PM-01	信息安全计划	不适用	-
PM-02	信息安全计划领导角色	不适用	-
PM-03	信息安全与隐私资源	不适用	-
PM-04	行动计划与里程碑流程	不适用	-
PM-05	系统清单	不适用	-
PM-05(01)	系统清单 | 个人可识别信息清单信息	不适用	-
PM-06	性能度量	不适用	-
PM-07	企业架构	不适用	-
PM-07(01)	企业架构 | 卸载	不适用	-
PM-08	关键基础设施计划	不适用	-
PM-09	风险管理策略	不适用	-
PM-10	授权流程	不适用	-
PM-11	使命与业务流程定义	不适用	-
PM-12	内部威胁计划	不适用	-
PM-13	安全与隐私工作人员	不适用	-
PM-14	测试、培训与监控	不适用	-
PM-15	安全与隐私组和协会	不适用	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PM-16	Threat Awareness Program	N/A	—
PM-16(01)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	N/A	—
PM-17	Protecting Controlled Unclassified Information on External Systems	N/A	—
PM-18	Privacy Program Plan	N/A	—
PM-19	Privacy Program Leadership Role	N/A	—
PM-20	Dissemination of Privacy Program Information	N/A	—
PM-20(01)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	N/A	—
PM-21	Accounting of Disclosures	N/A	—
PM-22	Personally Identifiable Information Quality Management	N/A	—
PM-23	Data Governance Body	N/A	—
PM-24	Data Integrity Board	N/A	—
PM-25	Minimization of PII Used in Testing, Training, and Research	N/A	—
PM-26	Complaint Management	N/A	—
PM-27	Privacy Reporting	N/A	—
PM-28	Risk Framing	N/A	—
PM-29	Risk Management Program Leadership Roles	N/A	—
PM-30	Supply Chain Risk Management Strategy	N/A	—
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-Essential Items	N/A	—
PM-31	Continuous Monitoring Strategy	N/A	—
PM-32	Purposing	N/A	—

Table 16. Personnel Security (PS)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PS-01	Policy and Procedures	CUI	03.15.01
PS-02	Position Risk Designation	FED	—
PS-03	Personnel Screening	CUI	03.09.01
PS-04	Personnel Termination	CUI	03.09.02
PS-05	Personnel Transfer	CUI	03.09.02
PS-06	Access Agreements	NCO	—
PS-07	External Personnel Security	NCO	—
PS-08	Personnel Sanctions	NCO	—
PS-09	Position Descriptions	FED	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PM-16	威胁意识计划	不适用	-
PM-16(01)	威胁意识计划 | 自动化共享手段威胁情报	不适用	-
PM-17	保护外部系统上的受控非机密信息系统	不适用	-
PM-18	隐私计划计划	不适用	-
PM-19	隐私计划领导角色	不适用	-
PM-20	隐私计划信息的传播	不适用	-
PM-20(01)	隐私计划信息的传播 | 隐私政策关于网站、应用程序和数字服务	不适用	-
PM-21	披露记录	不适用	-
PM-22	个人可识别信息质量管理	不适用	-
PM-23	数据治理机构	不适用	-
PM-24	数据完整性委员会	不适用	-
PM-25	测试、培训和研究中所用PII的最小化	不适用	-
PM-26	投诉管理	不适用	-
PM-27	隐私报告	不适用	-
PM-28	风险框架	不适用	-
PM-29	风险管理项目领导角色	不适用	-
PM-30	供应链风险管理策略	不适用	-
PM-30(01)	供应链风险管理策略 | 关键供应商或任务必需项	不适用	-
PM-31	持续监控策略	不适用	-
PM-32	目的设定	不适用	-

表 16. 人员安全(PS)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PS-01	策略与程序	CUI	03.15.01
PS-02	岗位风险指定	FED	-
PS-03	人员筛查	CUI	03.09.01
PS-04	人员解聘	CUI	03.09.02
PS-05	人员调动	CUI	03.09.02
PS-06	访问协议	NCO	-
PS-07	外部人员安全	NCO	-
PS-08	人员制裁	NCO	-
PS-09	岗位描述	FED	-

Table 17. PII Processing and Transparency (PT)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
PT-01	Policy and Procedures	N/A	—
PT-02	Authority to Process Personally Identifiable Information	N/A	—
PT-02(01)	Authority to Process Personally Identifiable Information | Data Tagging	N/A	—
PT-02(02)	Authority to Process Personally Identifiable Information | Automation	N/A	—
PT-03	Personally Identifiable Information Processing Purposes	N/A	—
PT-03(01)	Personally Identifiable Information Processing Purposes | Data Tagging	N/A	—
PT-03(02)	Personally Identifiable Information Processing Purposes | Automation	N/A	—
PT-04	Consent	N/A	—
PT-04(01)	Consent | Tailored Consent	N/A	—
PT-04(02)	Consent | Just-in-Time Consent	N/A	—
PT-04(03)	Consent | Revocation	N/A	—
PT-05	Privacy Notice	N/A	—
PT-05(01)	Privacy Notice | Just-in-Time Notice	N/A	—
PT-05(02)	Privacy Notice | Privacy Act Statements	N/A	—
PT-06	System of Records Notice	N/A	—
PT-06(01)	System of Records Notice | Routine Uses	N/A	—
PT-06(02)	System of Records Notice | Exemption Rules	N/A	—
PT-07	Specific Categories of Personally Identifiable Information	N/A	—
PT-07(01)	Specific Categories of Personally Identifiable Information | Social Security Numbers	N/A	—
PT-07(02)	Specific Categories of Personally Identifiable Information | First Amendment Information	N/A	—
PT-08	Computer Matching Requirements	N/A	—

Table 18. Risk Assessment (RA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
RA-01	Policy and Procedures	CUI	03.15.01
RA-02	Security Categorization	FED	—
RA-03	Risk Assessment	CUI	03.11.01
RA-03(01)	Risk Assessment | Supply Chain Risk Assessment	CUI	03.11.01
RA-05	Vulnerability Monitoring and Scanning	CUI	03.11.02
RA-05(02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned	CUI	03.11.02
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access	ORC	—

表 17. PII处理和透明度(PT)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
PT-01	策略与程序	不适用	-
PT-02	处理个人可识别信息的权限	不适用	-
PT-02(01)	处理个人可识别信息的权限 | 数据标记	不适用	-
PT-02(02)	处理个人可识别信息的权限 | 自动化	不适用	-
PT-03	个人可识别信息处理目的	不适用	-
PT-03(01)	个人可识别信息处理目的 | 数据标记	不适用	-
PT-03(02)	个人可识别信息处理目的 | 自动化	不适用	-
PT-04	同意	不适用	-
PT-04(01)	同意 | 定制同意	不适用	-
PT-04(02)	同意 | 即时同意	不适用	-
PT-04(03)	同意 | 撤销	不适用	-
PT-05	隐私声明	不适用	-
PT-05(01)	隐私声明 | 即时通知	不适用	-
PT-05(02)	隐私声明 | 隐私法声明	不适用	-
PT-06	记录系统通知	不适用	-
PT-06(01)	记录系统通知 | 常规用途	不适用	-
PT-06(02)	记录系统通知 | 豁免规则	不适用	-
PT-07	特定类别的个人可识别信息	不适用	-
PT-07(01)	特定类别的个人可识别信息 | 社交安全编号	不适用	-
PT-07(02)	特定类别的个人可识别信息 | 第一修订信息	不适用	-
PT-08	计算机匹配要求	不适用	-

表 18. 风险评估(RA)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
RA-01	策略与程序	CUI	03.15.01
RA-02	安全分类	FED	-
RA-03	风险评估	CUI	03.11.01
RA-03(01)	风险评估 | 供应链风险评估	CUI	03.11.01
RA-05	脆弱性监控与扫描	CUI	03.11.02
RA-05(02)	漏洞监控与扫描 | 更新漏洞待扫描	CUI	03.11.02
RA-05(05)	漏洞监控与扫描 | 特权访问	ORC	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
RA-05(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	NCO	—
RA-07	Risk Response	CUI	03.11.04
RA-09	Criticality Analysis	NCO	—

Table 19. System and Services Acquisition (SA)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SA-01	Policy and Procedures	CUI	03.15.01
SA-02	Allocation of Resources	NCO	—
SA-03	System Development Life Cycle	NCO	—
SA-04	Acquisition Process	NCO	—
SA-04(01)	Acquisition Process | Functional Properties of Controls	NCO	—
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	NCO	—
SA-04(09)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	NCO	—
SA-04(10)	Acquisition Process | Use of Approved PIV Products	FED	—
SA-05	System Documentation	NCO	—
SA-08	Security and Privacy Engineering Principles	CUI	03.16.01
SA-09	External System Services	CUI	03.16.03
SA-09(02)	External System Services | Identification of Functions, Ports, Protocols, and Services	ORC	—
SA-10	Developer Configuration Management	NCO	—
SA-11	Developer Testing and Evaluation	NCO	—
SA-15	Development Process, Standards, and Tools	NCO	—
SA-15(03)	Development Process, Standards, and Tools | Criticality Analysis	NCO	—
SA-22	Unsupported System Components	CUI	03.16.02

Table 20. System and Communications Protection (SC)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SC-01	Policy and Procedures	CUI	03.15.01
SC-02	Separation of System and User Functionality	ORC	—
SC-04	Information in Shared System Resources	CUI	03.13.04
SC-05	Denial-of-Service Protection	NCO	—
SC-07	Boundary Protection	CUI	03.13.01
SC-07(03)	Boundary Protection | Access Points	ORC	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
RA-05(11)	漏洞监控与扫描 | 公开披露计划	NCO	-
RA-07	风险响应	CUI	03.11.04
RA-09	关键性分析	NCO	-

表 19. 系统和服务获取(SA)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
SA-01	策略与程序	CUI	03.15.01
SA-02	资源分配	NCO	-
SA-03	系统开发生命周期	NCO	-
SA-04	获取流程	NCO	-
SA-04(01)	采购流程 | 控制措施的功能属性	NCO	-
SA-04(02)	采购流程 | 设计与实施信息用于控制措施	NCO	-
SA-04(09)	采购流程 | 功能、端口、协议和服务在使用	NCO	-
SA-04(10)	采购流程 | 使用经批准的 PIV 产品	FED	-
SA-05	系统文档	NCO	-
SA-08	安全与隐私工程原则	CUI	03.16.01
SA-09	外部系统服务	CUI	03.16.03
SA-09(02)	外部系统服务 | 功能、端口、协议和服务	ORC	-
SA-10	开发者配置管理	NCO	-
SA-11	开发者测试与评估	NCO	-
SA-15	开发过程、标准与工具	NCO	-
SA-15(03)	开发过程、标准与工具 | 关键性分析	NCO	-
SA-22	不支持的系统组件	CUI	03.16.02

表 20. 系统和通信保护(SC)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
SC-01	策略与程序	CUI	03.15.01
SC-02	系统与用户功能分离	ORC	-
SC-04	共享系统资源中的信息	CUI	03.13.04
SC-05	拒绝服务保护	NCO	-
SC-07	边界保护	CUI	03.13.01
SC-07(03)	边界保护 | 接入点	ORC	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SC-07(04)	Boundary Protection | External Telecommunications Services	ORC	—
SC-07(05)	Boundary Protection | Deny by Default – Allow by Exception	CUI	03.13.06
SC-07(07)	Boundary Protection | Split Tunneling for Remote Devices	ORC	—
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	ORC	—
SC-08	Transmission Confidentiality and Integrity	CUI	03.13.08
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	CUI	03.13.08
SC-10	Network Disconnect	CUI	03.13.09
SC-12	Cryptographic Key Establishment and Management	CUI	03.13.10
SC-13	Cryptographic Protection	CUI	03.13.11
SC-15	Collaborative Computing Devices and Applications	CUI	03.13.12
SC-17	Public Key Infrastructure Certificates	FED	—
SC-18	Mobile Code	CUI	03.13.13
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	NCO	—
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NCO	—
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NCO	—
SC-23	Session Authenticity	CUI	03.13.15
SC-28	Protection of Information at Rest	CUI	03.13.08
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	CUI	03.13.08
SC-39	Process Isolation	NCO	—

Table 21. System and Information Integrity (SI)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SI-01	Policy and Procedures	CUI	03.15.01
SI-02	Flaw Remediation	CUI	03.14.01
SI-02(02)	Flaw Remediation | Automated Flaw Remediation Status	NCO	—
SI-03	Malicious Code Protection	CUI	03.14.02
SI-04	System Monitoring	CUI	03.14.06
SI-04(02)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	NCO	—
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic	CUI	03.14.06
SI-04(05)	System Monitoring | System-Generated Alerts	NCO	—
SI-05	Security Alerts, Advisories, and Directives	CUI	03.14.03
SI-07	Software, Firmware, and Information Integrity	NCO	—
SI-07(01)	Software, Firmware, and Information Integrity | Integrity Checks	NCO	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
SC-07(04)	边界保护 | 外部电信服务	ORC	-
SC-07(05)	边界保护 | 默认拒绝 - 例外允许 CUI 03.13.06		
SC-07(07)	边界保护 | 远程设备的拆分隧道	ORC	-
SC-07(08)	边界保护 | 将流量路由至经过身份验证的代理服务器	ORC	-
SC-08	传输机密性与完整性	CUI 03.13.08	
SC-08(01)	传输机密性和完整性 | 加密保护	CUI 03.13.08	
SC-10	网络断开	CUI 03.13.09	
SC-12	加密密钥建立与管理	CUI 03.13.10	
SC-13	加密保护	CUI 03.13.11	
SC-15	协作计算设备与应用程序	CUI 03.13.12	
SC-17	公钥基础设施证书	FED	-
SC-18	移动代码	CUI 03.13.13	
SC-20	安全名称/地址解析服务(权威源)	NCO	-
SC-21	安全名称/地址解析服务(递归或缓存)解析器)	NCO	-
SC-22	名称/地址解析的架构与配置服务	NCO	-
SC-23	会话真实性	CUI 03.13.15	
SC-28	静态信息保护	CUI 03.13.08	
SC-28(01)	静态信息保护 | 密码保护 CUI 03.13.08		
SC-39	进程隔离	NCO	-

表 21. 系统和信息完整性(SI)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
SI-01	策略与程序	CUI 03.15.01	
SI-02	缺陷修复	CUI 03.14.01	
SI-02(02)	缺陷修复 | 自动化缺陷修复状态	NCO	-
SI-03	恶意代码防护	CUI 03.14.02	
SI-04	系统监控	CUI 03.14.06	
SI-04(02)	系统监控 | 用于实时监控的自动化工具和机制时间分析	NCO	-
SI-04(04)	系统监控 | 入站和出站通信流量	CUI 03.14.06	
SI-04(05)	系统监控 | 系统生成的警报	NCO	-
SI-05	安全警报、公告和指令	CUI 03.14.03	
SI-07	软件、固件和信息完整性	NCO	-
SI-07(01)	软件、固件和信息完整性 | 完整性检查	NCO	-

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SI-07(07)	Software, Firmware, and Information Integrity | Integration of Detection and Response	NCO	—
SI-08	Spam Protection	ORC	—
SI-08(02)	Spam Protection | Automatic Updates	NCO	—
SI-10	Information Input Validation	NCO	—
SI-11	Error Handling	NCO	—
SI-12	Information Management and Retention	CUI	03.14.08
SI-16	Memory Protection	NCO	—

Table 22. Supply Chain Risk Management (SR)

NIST SP 800-53 CONTROLS MODERATE BASELINE		TAILORING CRITERIA	SECURITY REQUIREMENT
SR-01	Policy and Procedures	CUI	03.15.01
SR-02	Supply Chain Risk Management Plan	CUI	03.17.01
SR-02(01)	Supply Chain Risk Management Plan | Establish SCRM Team	NCO	—
SR-03	Supply Chain Controls and Processes	CUI	03.17.03
SR-05	Acquisition Strategies, Tools, and Methods	CUI	03.17.02
SR-06	Supplier Assessments and Reviews	CUI	03.11.01
SR-08	Notification Agreements	NCO	—
SR-10	Inspection of Systems or Components	NCO	—
SR-11	Component Authenticity	NCO	—
SR-11(01)	Component Authenticity | Anti-Counterfeit Training	NCO	—
SR-11(02)	Component Authenticity | Configuration Control for Component Service and Repair	NCO	—
SR-12	Component Disposal	ORC	—

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
SI-07(07)	软件、固件和信息完整性 | 集成检测与响应	NCO	-
SI-08	垃圾邮件防护	ORC	-
SI-08(02)	垃圾邮件防护 | 自动更新	NCO	-
SI-10	信息输入验证	NCO	-
SI-11	错误处理	NCO	-
SI-12	信息管理与保留	CUI	03.14.08
SI-16	内存保护	NCO	-

表 22. 供应链风险管理(SR)

NIST SP 800-53 控制措施中等基线		裁剪标准	安全要求
SR-01	策略与程序	CUI	03.15.01
SR-02	供应链风险管理计划	CUI	03.17.01
SR-02(01)	供应链风险管理计划 | 建立 SCRM 团队	NCO	-
SR-03	供应链控制与流程	CUI	03.17.03
SR-05	采购策略、工具和方法	CUI	03.17.02
SR-06	供应商评估与审查	CUI	03.11.01
SR-08	通知协议	NCO	-
SR-10	系统或组件检查	NCO	-
SR-11	组件真实性	NCO	-
SR-11(01)	组件真实性 | 防伪培训	NCO	-
SR-11(02)	组件真实性 | 组件配置控制服务与维修	NCO	-
SR-12	组件处置	ORC	-

Appendix D. Organization-Defined Parameters

This appendix lists the organization-defined parameters (ODPs) that are included in the security requirements in Sec. 3. The ODPs are listed sequentially by requirement family, beginning with the first requirement containing an ODP in the Access Control (AC) family and ending with the last requirement containing an ODP in the Supply Chain Risk Management (SR) family.

Table 23. Organization-Defined Parameters

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.01	03.01.01.f.02	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.g.01	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.g.02	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.g.03	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.h	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.h	[*Assignment: organization-defined circumstances*]
03.01.05	03.01.05.b	[*Assignment: organization-defined security functions*]
03.01.05	03.01.05.b	[*Assignment: organization-defined security-relevant information*]
03.01.05	03.01.05.c	[*Assignment: organization-defined frequency*]
03.01.06	03.01.06.a	[*Assignment: organization-defined personnel or roles*]
03.01.08	03.01.08.a	[*Assignment: organization-defined number*]
03.01.08	03.01.08.a	[*Assignment: organization-defined time period*]
03.01.08	03.01.08.a	[*Assignment: organization-defined time period*]
03.01.08	03.01.08.b	[*Selection (one or more): lock the account or node for an* [*Assignment: organization-defined time period*]*; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action*]
03.01.10	03.01.10.a	[*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]
03.01.11	03.01.11	[*Assignment: organization-defined conditions or trigger events requiring session disconnect*]
03.01.20	03.01.20.b	[*Assignment: organization-defined security requirements*]
03.02.01	03.02.01.a.01	[*Assignment: organization-defined frequency*]
03.02.01	03.02.01.a.02	[*Assignment: organization-defined events*]
03.02.01	03.02.01.b	[*Assignment: organization-defined frequency*]
03.02.01	03.02.01.b	[*Assignment: organization-defined events*]
03.02.02	03.02.02.a.01	[*Assignment: organization-defined frequency*]
03.02.02	03.02.02.a.02	[*Assignment: organization-defined events*]
03.02.02	03.02.02.b	[*Assignment: organization-defined frequency*]
03.02.02	03.02.02.b	[*Assignment: organization-defined events*]
03.03.01	03.03.01.a	[*Assignment: organization-defined event types*]
03.03.01	03.03.01.b	[*Assignment: organization-defined frequency*]
03.03.04	03.03.04.a	[*Assignment: organization-defined time period*]

附录 D.组织定义的参数

本附录列出了第 3 节安全要求中包含的组织定义参数(ODP)。ODP 按需求族顺序列出，从访问控制(AC)族中包含 ODP 的第一个需求开始，到供应链风险管理(SR)族中包含 ODP 的最后一个需求结束。

表 23. 组织定义的参数

安全要求	组织定义参数	
03.01.01	03.01.01.f.02	[分配：组织定义的时间段]
03.01.01	03.01.01.g.01	[分配：组织定义的时间段]
03.01.01	03.01.01.g.02	[分配：组织定义的时间段]
03.01.01	03.01.01.g.03	[分配：组织定义的时间段]
03.01.01	03.01.01.h	[分配：组织定义的时间段]
03.01.01	03.01.01.h	[分配：组织定义的情况]
03.01.05	03.01.05.b	[分配：组织定义的安全功能]
03.01.05	03.01.05.b	[分配：组织定义的安全相关信息]
03.01.05	03.01.05.c	[分配：组织定义的频率]
03.01.06	03.01.06.一个	[分配：组织定义的人员或角色]
03.01.08	03.01.08.一个	[分配：组织定义的编号]
03.01.08	03.01.08.一个	[分配：组织定义的时间段]
03.01.08	03.01.08.b	[选择*(*一项或多项*)*：锁定账户或节点[赋值：组织定义的时间段] ；锁定账户或节点直至管理员释放；延迟下一次登录提示；通知系统管理员；采取其他措施]
03.01.10	03.01.10.a	[选择*(*一项或多项*)*：在[赋值：组织定义的时间段] 不活动后启动设备锁定；要求用户在离开系统无人看管前启动设备锁定]
03.01.11	03.01.11	[赋值：组织定义的需断开会话的条件或触发事件]
03.01.20	03.01.20.b	[分配：组织定义的安全要求]
03.02.01	03.02.01.a.01	[分配：组织定义的频率]
03.02.01	03.02.01.a.02	[分配：组织定义的事件]
03.02.01	03.02.01.b	[分配：组织定义的频率]
03.02.01	03.02.01.b	[分配：组织定义的事件]
03.02.02	03.02.02.a.01	[分配：组织定义的频率]
03.02.02	03.02.02.a.02	[分配：组织定义的事件]
03.02.02	03.02.02.b	[分配：组织定义的频率]
03.02.02	03.02.02.b	[分配：组织定义的事件]
03.03.01	03.03.01.一个	[分配：组织定义的事件类型]
03.03.01	03.03.01.b	[分配：组织定义的频率]
03.03.04	03.03.04.一个	[分配：组织定义的时间段]

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.03.04	03.03.04.b	[*Assignment: organization-defined additional actions*]
03.03.05	03.03.05.a	[*Assignment: organization-defined frequency*]
03.03.07	03.03.07.b	[*Assignment: organization-defined granularity of time measurement*]
03.04.01	03.04.01.b	[*Assignment: organization-defined frequency*]
03.04.02	03.04.02.a	[*Assignment: organization-defined configuration settings*]
03.04.06	03.04.06.b	[*Assignment: organization-defined functions, ports, protocols, connections, and/or services*]
03.04.06	03.04.06.c	[*Assignment: organization-defined frequency*]
03.04.08	03.04.08.c	[*Assignment: organization-defined frequency*]
03.04.10	03.04.10.b	[*Assignment: organization-defined frequency*]
03.04.12	03.04.12.a	[*Assignment: organization-defined system configurations*]
03.04.12	03.04.12.b	[*Assignment: organization-defined security requirements*]
03.05.01	03.05.01.b	[*Assignment: organization-defined circumstances or situations requiring re-authentication*]
03.05.02	03.05.02	[*Assignment: organization-defined devices or types of devices*]
03.05.05	03.05.05.c	[*Assignment: organization-defined time period*]
03.05.05	03.05.05.d	[*Assignment: organization-defined characteristic identifying individual status*]
03.05.07	03.05.07.a	[*Assignment: organization-defined frequency*]
03.05.07	03.05.07.f	[*Assignment: organization-defined composition and complexity rules*]
03.05.12	03.05.12.e	[*Assignment: organization-defined frequency*]
03.05.12	03.05.12.e	[*Assignment: organization-defined events*]
03.06.02	03.06.02.b	[*Assignment: organization-defined time period*]
03.06.02	03.06.02.c	[*Assignment: organization-defined authorities*]
03.06.03	03.06.03	[*Assignment: organization-defined frequency*]
03.06.04	03.06.04.a.01	[*Assignment: organization-defined time period*]
03.06.04	03.06.04.a.03	[*Assignment: organization-defined frequency*]
03.06.04	03.06.04.b	[*Assignment: organization-defined frequency*]
03.06.04	03.06.04.b	[*Assignment: organization-defined events*]
03.08.07	03.08.07.a	[*Assignment: organization-defined types of system media*]
03.09.01	03.09.01.b	[*Assignment: organization-defined conditions requiring rescreening*]
03.09.02	03.09.02.a.01	[*Assignment: organization-defined time period*]
03.10.01	03.10.01.c	[*Assignment: organization-defined frequency*]
03.10.02	03.10.02.b	[*Assignment: organization-defined frequency*]
03.10.02	03.10.02.b	[*Assignment: organization-defined events or potential indications of events*]
03.10.06	03.10.06.b	[*Assignment: organization-defined security requirements*]
03.11.01	03.11.01.b	[*Assignment: organization-defined frequency*]
03.11.02	03.11.02.a	[*Assignment: organization-defined frequency*]
03.11.02	03.11.02.b	[*Assignment: organization-defined response times*]
03.11.02	03.11.02.c	[*Assignment: organization-defined frequency*]

安全要求	组织定义参数	
03.03.04	03.03.04.b	[分配：组织定义的附加操作]
03.03.05	03.03.05.一个	[分配：组织定义的频率]
03.03.07	03.03.07.b	[赋值：组织定义的时间测量粒度]
03.04.01	03.04.01.b	[分配：组织定义的频率]
03.04.02	03.04.02.一个	[分配：组织定义的配置设置]
03.04.06	03.04.06.b	[分配：组织定义的 *functions*、端口、协议、连接和/或服务]
03.04.06	03.04.06.c	[分配：组织定义的频率]
03.04.08	03.04.08.c	[分配：组织定义的频率]
03.04.10	03.04.10.b	[分配：组织定义的频率]
03.04.12	03.04.12.一个	[分配：组织定义的系统配置]
03.04.12	03.04.12.b	[分配：组织定义的安全要求]
03.05.01	03.05.01.b	[赋值：组织定义的需重新身份验证的情况或情形]
03.05.02	03.05.02	[分配：组织定义的设备或设备类型]
03.05.05	03.05.05.c	[分配：组织定义的时间段]
03.05.05	03.05.05.d	[赋值：组织定义的标识个人状态的特性]
03.05.07	03.05.07.一个	[分配：组织定义的频率]
03.05.07	03.05.07.f	[分配：组织定义的组成和复杂性规则]
03.05.12	03.05.12.e	[分配：组织定义的频率]
03.05.12	03.05.12.e	[分配：组织定义的事件]
03.06.02	03.06.02.b	[分配：组织定义的时间段]
03.06.02	03.06.02.c	[分配：组织定义的权限机构]
03.06.03	03.06.03	[分配：组织定义的频率]
03.06.04	03.06.04.a.01	[分配：组织定义的时间段]
03.06.04	03.06.04.a.03	[分配：组织定义的频率]
03.06.04	03.06.04.b	[分配：组织定义的频率]
03.06.04	03.06.04.b	[分配：组织定义的事件]
03.08.07	03.08.07.一个	[分配：组织定义的系统介质类型]
03.09.01	03.09.01.b	[分配：组织定义的需重新筛查的条件]
03.09.02	03.09.02.a.01	[分配：组织定义的时间段]
03.10.01	03.10.01.c	[分配：组织定义的频率]
03.10.02	03.10.02.b	[分配：组织定义的频率]
03.10.02	03.10.02.b	[赋值：组织定义的事件或事件的潜在迹象]
03.10.06	03.10.06.b	[分配：组织定义的安全要求]
03.11.01	03.11.01.b	[分配：组织定义的频率]
03.11.02	03.11.02.一个	[分配：组织定义的频率]
03.11.02	03.11.02.b	[分配：组织定义的响应时间]
03.11.02	03.11.02.c	[分配：组织定义的频率]

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.12.01	03.12.01	[*Assignment: organization-defined frequency*]
03.12.05	03.12.05.a	[*Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; nondisclosure agreements; other types of agreements*]
03.12.05	03.12.05.c	[*Assignment: organization-defined frequency*]
03.13.09	03.13.09	[*Assignment: organization-defined time period*]
03.13.10	03.13.10	[*Assignment: organization-defined requirements for key establishment and management*]
03.13.11	03.13.11	[*Assignment: organization-defined types of cryptography*]
03.13.12	03.13.12.a	[*Assignment: organization-defined exceptions where remote activation is to be allowed*]
03.14.01	03.14.01.b	[*Assignment: organization-defined time period*]
03.14.02	03.14.02.c.01	[*Assignment: organization-defined frequency*]
03.15.01	03.15.01.b	[*Assignment: organization-defined frequency*]
03.15.02	03.15.02.b	[*Assignment: organization-defined frequency*]
03.15.03	03.15.03.d	[*Assignment: organization-defined frequency*]
03.16.01	03.16.01	[*Assignment: organization-defined systems security engineering principles*]
03.16.03	03.16.03.a	[*Assignment: organization-defined security requirements*]
03.17.01	03.17.01.b	[*Assignment: organization-defined frequency*]
03.17.03	03.17.03.b	[*Assignment: organization-defined security requirements*]

安全要求	组织定义参数	
03.12.01	03.12.01	[分配：组织定义的频率]
03.12.05	03.12.05.一个	[选择(一项或多项)：互连安全协议；信息交换安全协议；谅解备忘录或协议；服务级别协议；用户协议；保密协议；其他类型的协议]
03.12.05	03.12.05.c	[分配：组织定义的频率]
03.13.09	03.13.09	[分配：组织定义的时间段]
03.13.10	03.13.10	[赋值：组织定义的密钥建立和管理要求]
03.13.11	03.13.11	[分配：组织定义的密码学类型]
03.13.12	03.13.12.一个	[赋值：组织定义的允许远程激活的例外情况]
03.14.01	03.14.01.b	[分配：组织定义的时间段]
03.14.02	03.14.02.c.01	[分配：组织定义的频率]
03.15.01	03.15.01.b	[分配：组织定义的频率]
03.15.02	03.15.02.b	[分配：组织定义的频率]
03.15.03	03.15.03.d	[分配：组织定义的频率]
03.16.01	03.16.01	[赋值：组织定义的系统安全工程原则]
03.16.03	03.16.03.一个	[分配：组织定义的安全要求]
03.17.01	03.17.01.b	[分配：组织定义的频率]
03.17.03	03.17.03.b	[分配：组织定义的安全要求]

Appendix E. Change Log

This publication incorporates the following changes from the original edition (February 2020; updated January 28, 2021):

- Streamlined introductory information in Sec. 1 and Sec. 2 to improve clarity and understanding
- Modified the security requirements and families in Sec. 3 to reflect the security controls in the SP 800-53B [12] moderate baseline and the tailoring actions in Appendix C
- Eliminated the distinction between basic and derived security requirements
- Increased the specificity of security requirements to remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments
- Introduced organization-defined parameters (ODPs) in selected security requirements to increase flexibility and help organizations better manage risk
- Grouped security requirements, where possible, to improve understanding and the efficiency of implementations and assessments
- Removed outdated and redundant security requirements
- Added new security requirements
- Added titles to the security requirements
- Restructured and streamlined the security requirement discussion sections
- Added new tailoring categories: Other Related Controls (ORC) and Not Applicable (N/A)
- Recategorized selected controls in the SP 800-53B moderate baseline using the tailoring criteria in Appendix C
- Revised the security requirements for consistency with the security control language in SP 800-53
- Revised the structure of the References, Acronyms, and Glossary sections for greater clarity and ease of use
- Revised the tailoring tables in Appendix C to be consistent with the changes to the security requirements
- Added new appendix listing organization-defined parameters for security requirements

Table 24 shows the changes incorporated into this publication. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates to this document that are not yet published in an errata update or a formal revision, including additional issues and potential corrections, will be posted as they are identified. See the publication details for this report. The current release of this publication does not include any errata updates.

附录 E.变更日志

本出版物纳入了对原始版本(2020 年 2 月；2021 年 1 月 28 日更新)的以下变更：

- 精简了第 1 节和第 2 节中的介绍性信息，以提高清晰度和理解度
- 修改了第3节中的安全要求和族，以反映SP 800-53B[12]中等基线中的安全控制以及附录C中的裁剪操作
- 消除了基本安全要求与派生安全要求之间的区别
- 提高了安全要求的具体性，以消除歧义、提高实施的有效性并明确评估范围
- 在选定的安全要求中引入了组织定义参数(ODP)，以增加灵活性并帮助组织更好地管理风险
- 在可能的情况下对安全要求进行分组，以提高理解以及实施和评估的效率
- 删除了过时和冗余的安全要求
- 新增了安全要求
- 为安全要求添加了标题
- 重构并简化了安全要求讨论部分
- 新增了裁剪类别：其他相关控制(ORC)和不适用(N/A)
- 使用附录C中的裁剪标准对SP 800-53B中等基线中的选定控制进行了重新分类
- 修订了安全要求，以与SP 800-53中的安全控制语言保持一致
- 修订了参考文献、缩略语和术语表部分的结构，以提高清晰度和易用性
- 修订了附录C中的裁剪表，以与安全要求的变更保持一致
- 新增了附录，列出安全要求的组织定义参数

表24显示了纳入本出版物的变更。勘误更新可包括出版物中在性质上属于编辑性或实质性的更正、澄清或其他细微变更。对本文件的任何潜在更新，若尚未在勘误更新或正式修订中发布，包括其他问题和潜在更正，将在识别后予以发布。参见本报告的出版物详细信息。本出版物的当前版本不包含任何勘误更新。

Table 24. Change Log

PUBLICATION ID	DATE	TYPE OF EDIT	CHANGE	LOCATION

表 24. 变更日志

出版物 ID	日期	编辑类型	变更	位置

How this file was made

This is a complete Chinese translation of NIST SP 800-171r3, Protecting Controlled Unclassified Information. Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/nist-800-171-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《保护受控非机密信息（SP 800-171r3）》的中文全译本，共 120 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/nist-800-171-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。