State of California

Department of Technology

Office of Information Security

Server Hardening Standard

SIMM 5355-B

October 2024

Revision History

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
v.1	October 2024	Office of Information Security	Initial Release

Purpose

Server hardening is the process of enhancing server security through a variety of methods and practices aimed at reducing vulnerabilities. This process involves assessment and fortification of server configurations, management of operating systems, and implementation of security measures.

The objective of server hardening is to maintain the integrity, confidentiality, and availability of data. Since security threats are constantly evolving, server hardening is a continuous process that demands consistent monitoring and updating to adapt to new security challenges and evolving threats.

This standard outlines the minimum baseline security standards necessary for server hardening. State entities are recommended to adopt additional context-specific controls where necessary.

Scope

The Server Hardening Standard applies to all California state entities, including agencies, departments, divisions, bureaus, boards, and commissions as defined in Government Code Section 11546.1.

Compliance

Government Code Section 11549.3 authorizes the Office of Information Security (OIS) to create, issue, and maintain policies, standards, and procedures; oversee information security risk management for state entities; provide information security and privacy guidance; and ensure compliance with State Administrative Manual (SAM) Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

State entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their entity. Non-compliance may affect audit findings and maturity metrics.

Definitions

- **Hardening** – A defense strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.
- **Least Privilege** – The principle that a security architecture is designed so that each

entity is granted the minimum system resources and authorizations that the entity needs to perform its function, and users are granted access to only those information assets they need to perform their official duties.

- **System Security Plan (SSP)** - A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Minimum Baseline Standards

The minimum baseline standards for server hardening follow the core functions of the NIST Cybersecurity Framework (CSF) 2.0. They enable entities to systematically approach and mitigate cybersecurity risk by governing, identifying, protecting, detecting, responding to, and recovering vulnerabilities and threats associated with server administration. Each requirement is mapped to the applicable CSF 2.0 category.

Note: The CSF 2.0 functions Respond and Recover are not applicable to the server hardening standards.

I. Govern

CSF Category	Requirement Description	Requirement
GV.RM Risk Management Strategy	Establish a risk management plan and conduct testing to understand the current state of your server security.	PM-4
GV.RR Roles, Responsibilities, and Authorities	Ensure security management staff are involved in server planning, implementation, and administration.	SA-3
GV.PO Policies, Processes, and Procedures	Create a System Security Plan (SSP)	PL-2

II. Identify

CSF Category	Requirement Description	Requirement
ID.AM Asset Management	Maintain inventories of hardware, software, services, and information systems managed by the organization. Prioritize assets based on classification, criticality, resources, and impact on the mission.	CM-8
	Ensure information systems, hardware,	SA-3

	software, and services are managed throughout their life cycle.	
ID.RA Risk Assessment	Develop and periodically update a plan of action and milestones and conduct risk assessments for the system to identify security gaps and the best ways to address them.	CA-5, RA-3

III. Protect

CSF Category	Requirement Description	Requirement
(PR.AA) Identity Management, Authentication, and Access Control	Verify identities and credentials for authorized users, services, and hardware are managed by the organization.	IA-5
	Ensure users, services, and hardware are authenticated.	IA-2
	Provide a host-based firewall capability to limit incoming and outgoing traffic, with a focus on securing nonsecure ports and protocols. This entails restricting the use of browsers on the server unless it is essential for its primary functions.	CM-7, CM-7(1), SC-7, SC-7(5), SC-8
	Incorporate the principles of least privilege, the ability to granularly restrict administrative or root-level activities to authorized users only, and the ability to granularly control access to data on the server.	AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(10), CM-5, CM-5(5)
	Confirm access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed. Typical files to which access should be restricted include: • Configuration files • Files related directly to security mechanisms (password hash files, cryptographic key materials, etc.), • System audit files • Security logs	AC-3, AC-3(7), AC-3(8), AC-3(11)
(PR.DS) Data Security	Implement support for strong authentication protocols and encryption algorithms.	AC-17, AC-18
	Use Federal Information Processing Standards (FIPS) validated cryptographic implementations when using cryptography to protect stored data and data communications.	AC-17, AC-17(2), SC-7, SC-7(4)
	Partition the system for physical or logical separation of components.	SC-32
(PR.PS) Platform Security	Apply secure baseline configuration (hardening), configuration management, and	CM-2, CM-3, CM-6, CM-6(1)

	change control best practices. The Resources section provides suggested baseline configuration resources.	
	Patch and update the Operating System (OS) and installed software.	SI-2, SI-2(4) SIMM 5345-A
	Perform frequent Vulnerability Scanning.	RA-5 SIMM 5345-A
	Configure Automated Time Synchronization.	SC-45
	Have DoS attack protection. This includes: • Control/configure the maximum number of server processes and/or network connections that the server should allow.	SC-5, SC-5(2), SC-5(3), SC-7, SC-7(3)
	Ensure software and hardware are maintained, replaced, and removed commensurate with risk.	MA-2
	Ensure installation and execution of unauthorized software is prevented.	CM-7, CM-7(2), CM-7(5)
	Configure warning banners to users before granting access to the system.	AC-8
(PR.IR) Technology Infrastructure Resilience	Ensure networks and environments are protected from threats and unauthorized physical and logical access/usage. Examples include: • Physical security protection mechanisms (Locks, card reader access, cameras, etc.) • Environmental controls (humidity and temperature controls, fire containment equipment, hardening against natural disasters) • Backup power (Uninterrupted Power Supply (UPS))	PE-3, PE-11, PE-13, PE-14
	Ensure servers are backed up periodically.	CP-9
	Perform occasional penetration testing.	CA-8

IV. Detect

CSF Category	Requirement Description	Requirement
DE.CM Continuous Monitoring	Ensure computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events. Note: State entities are recommended to use CDT's statewide SOC as a Service (SOCaaS) if they do not have 24/7 monitoring capabilities.	CA-7, CA-7(4) SIMM 5355-A

References

1. NIST Special Publication 800-123, Guide to General Server Security
   https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

2. NIST Publication 800-53 rev5, Security and Privacy Controls for Information Systems and Organizations
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

3. NIST Cybersecurity Framework 2.0
   https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

4. NIST Special Publication 800-171 rev2, Overview of Security Controls
   https://csf.tools/controlset/nist800-171r2/

5. NIST Special Publication 800-18 rev1, Guide for Developing Security Plans for Federal Information Systems
   https://csrc.nist.gov/pubs/sp/800/18/r1/final

6. SAM 4983.1 Cloud Computing Policy
   https://www.dgs.ca.gov/Resources/SAM/TOC/4900/4983-1

7. SIMM 140 Cloud Security Guide
   https://cdt.ca.gov/wp-content/uploads/2023/10/SIMM-140-Cloud-Security-Guide-1.docx

8. SIMM 5305-A Information Security Program Management Standard
   https://cdt.ca.gov/wp-content/uploads/2023/12/SIMM-5305_A_2023-12.pdf

9. SIMM 5345-A - Vulnerability Management Standard
   https://cdt.ca.gov/wp-content/uploads/2021/04/SIMM5345-A-Vulnerability_2021-0407_PT.pdf

10. SIMM 5355-A - Endpoint Protection Standard
    https://cdt.ca.gov/wp-content/uploads/2019/01/SIMM-5355-A.pdf

11. Federal Information Processing Standards, Standards for Security Categorization of Federal Information, and Information Systems (FIPS 199)
    https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

Baseline Configuration Resources

1. CIS Benchmarks – https://www.cisecurity.org/cis-benchmarks

2. DoD Security Technical Implementation Guides (Group Policy Objects) – https://public.cyber.mil/stigs/gpo/

3. MS Intune Security Baseline – https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines

APPENDIX A – SUMMARY OF CONTROLS

NIST Cybersecurity Framework & 800-53 Controls		
Govern	GV.RM: Risk Management Strategy	PM-4: Plan of Action and Milestones Process
	GV.RR: Roles, Responsibilities, and Authorities	SA-3: System Development Life Cycle
	GV.PO: Policies, Processes, and Procedures	PL-2: System Security and Privacy Plans NIST 800-18: Guide for Developing Security Plans for Federal Information Systems
Identify	ID.AM: Asset Management	CM-8: System Component Inventory
		SA-3: System Development Life Cycle
	ID.RA: Risk Assessment	CA-5: Plan of Action and Milestones
		RA-3: Risk Assessment
Protect	PR.AA: Identity Management, Authentication, and Access Control	AC-3: Access Enforcement • AC-3(7) Role-based Access Control • AC-3(8) Revocation of Access Authorizations • AC-3(11) Restrict Access to Specific Information Types
		AC-6: Least Privilege • AC-6(1) Authorize Access to Security Functions • AC-6(2) Non-privileged Access for Non-security Functions • AC-6(5) Privileged Accounts • AC-6(10) Prohibit Non-privileged Users from Executing Privileged
		CM-5: Access Restrictions for Change • CM-5(5) Privilege Limitation for Production and Operation
		CM-7: Least Functionality • CM-7(1) Periodic Review
		IA-2: Identification And Authentication
		IA-5: Authenticator Management
		SC-7: Boundary Protection • SC-7(5) Deny by Default — Allow by Exception
		SC-8: Transmission Confidentiality and Integrity
	PR.DS: Data Security	AC-17: Remote Access • AC-17(2) Protection of Confidentiality and Integrity Using Encryption

		AC-18: Wireless Access
		SC-7: Boundary Protection • SC-7(4) External Telecommunications Services
		SC-32: System Partitioning
	PR.PS: Platform Security	AC-8: System Use Notification
		AC-17: Remote Access • AC-17(2) Protection of Confidentiality and Integrity Using Encryption
		AC-18: Wireless Access
		CM-2: Baseline Configuration
		CM-3: Configuration Change Control
		CM-6: Configuration Settings • CM-6(1) Automated Management, Application, and Verification
		CM-7: Least Functionality • CM-7(2) Prevent Program Execution • CM-7(5) Authorized Software — Allow-by-exception
		MA-2: Controlled Maintenance
		RA-5: Vulnerability Monitoring and Scanning
		SC-5: Denial Of Service Protection • SC-5(2) Capacity, Bandwidth, and Redundancy • SC-5(3) Detection and Monitoring
		SC-7: Boundary Protection • SC-7(3) Access Points
		SC-32: System Partitioning
		SC-45: System Time Synchronization
		SI-2: Flaw Remediation • SI-2(4) Automated Patch Management Tools
		SIMM 5345-A: Vulnerability Management Standard
	PR.IR: Technology Infrastructure Resilience	CA-8: Penetration Testing
		CP-9: System Backup
		PE-3: Physical Access Control
		PE-11: Emergency Power
		PE-13: Fire Protection
		PE-14: Environmental Controls
Detect	DE.CM: Continuous Monitoring	CA-7: Continuous Monitoring • CA-7(4) Risk Monitoring