STATERAMP SECURITY CONTROLS

BASELINE SUMMARY

VERSION:
1.2
DATE:
April 29, 2022

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
10/29/2020	Original Publication	1.0	StateRAMP Steering Committee
01/08/2021	Update CSP definition	1.1	StateRAMP Staff
04/29/2022	Minor Updates to Baseline Controls	1.2	StateRAMP Standards and Technical Committee and Board

This document will be reviewed at the discretion of the StateRAMP Board a frequency no less than annually.

1. SELECTING A SECURITY CATEGORY

Once a state or local government and/or service provider has decided to require or pursue a StateRAMP status, the first step is to identify the required impact level. NIST SP 800-60, Rev 1 maps data sensitivity to impact levels, including low impact (generally public data), moderate impact (generally confidential data), and high impact (generally affecting national security). Most state and local government data will likely fit within low or moderate impact levels.

StateRAMP Security Controls are defined in three categories:

Low: Aligned with NIST Low Impact Control Baselines

Low+: Aligned with NIST Low Impact Control Baselines, with additional Moderate Impact Control Baselines for added security

Moderate: Aligned with NIST Moderate Control Baselines

It is the goal of StateRAMP to provide the state or local government Authorizing Body flexibility to require additional controls as appropriate. For example, additional controls may be necessary to comply with CJIS or MARS-E 2.0 requirements. These additional controls would be noted as (+) on the StateRAMP Authorized Product List (APL) so that service providers can benefit from the higher authorization indicating an ability to comply with more rigorous standards.

2. ABOUT THE SECURITY CONTROL BASELINES

StateRAMP developed the baseline with input from State officials, service providers, and security experts. The Baseline Controls are reviewed annually by the StateRAMP Standards and Technical Committee with annual updates recommended to the Board. It is the goal of StateRAMP to help mature and grow the service provider community and in doing so, improve the security profile of state and local governments, public education institutions and special districts. StateRAMP will verify that the service provider meets the intent of the security requirements as appropriate and fit for purpose.

All of the security controls listed in the table below are outlined in NIST 800-53 Rev. 4 . StateRAMP has published a Data Classification Tool to help guide the determination of Security Impact Level. As always, final determination lies with the contracting government information security official. The Data Classification Tool and StateRAMP Security Baseline Controls Templates are published and maintained on www.stateramp.org.

Summary of Required Security Controls

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
AC	**Access Control**				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1	AC-1
AC-2	Account Management *Only required for privileged accounts	AC-2	AC-2 (1) (7)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4 (21)	AC-4 (8) (21)
AC-5	Separation of Duties	Not Selected	AC-5	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (7) (8) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7	AC-7 (2)
AC-8	System Use Notification	AC-8	AC-8	AC-8	AC-8
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11 (1)	AC-11 (1)
AC-12	Session Termination *Only required for admin. back-end access	Not Selected	AC-12*	AC-12	AC-12 (1)
AC-14	Permitted Actions Without Identification or Authentication	AC-14	AC-14	AC-14	AC-14
AC-17	Remote Access	AC-17	AC-17 (1) (2) (9)	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)
AC-18	Wireless Access *Only required for on-premise solutions, so long as SaaS/PaaS host meets requirements	AC-18*	AC-18	AC-18 (1)	AC-18 (1) (3) (4) (5)
AC-19	Access Control For Mobile Devices	AC-19	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	Not Selected	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content *FedRAMP requires	Not Selected*	Not Selected	AC-22	AC-22

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
	AC-22 for Low Impact. It is not required as a baseline control for StateRAMP.				
AT	**Awareness and Training**				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	AT-2	AT-2 (2)	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	AT-3	AT-3	AT-3	AT-3 (3) (4)
AT-4	Security Training Records	AT-4	AT-4	AT-4	AT-4
AU	**Audit and Accountability**				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2	AU-2 (3)	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis and Reporting	AU-6	AU-6 (1)	AU-6 (1) (3)	AU-6 (1) (3) (4) (5) (6) (7) (10)
AU-7	Audit Reduction and Report Generation	Not Selected	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8 (1)	AU-8 (1)	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9 (2) (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12	AU-12 (1) (3)
CA	**Security Assessment and Authorization**				
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1)	CA-2 (1) (2) (3)	CA-2 (1) (2) (3)
CA-3	System Interconnections	CA-3	CA-3	CA-3 (5)	CA-3 (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)	CA-7 (1)	CA-7 (1) (3)

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
CA-8	Penetration Testing	Not Selected	CA-8 (1)	CA-8 (1)	CA-8 (1)
CA-9	Internal System Connections	CA-9	CA-9	CA-9	CA-9
CM	**Configuration Management**				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3)	CM-2 (1) (2) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (2)	CM-3 (1) (2) (4) (6)
CM-4	Security Impact Analysis	CM-4	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions For Change	Not Selected	CM-5	CM-5 (1) (3) (5)	CM-5 (1) (2) (3) (5)
CM-6	Configuration Settings	CM-6	CM-6 (1)	CM-6 (1)	CM-6 (1) (2)
CM-7	Least Functionality	CM-7	CM-7	CM-7 (1) (2) (5)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	CM-8 (1)	CM-8 (1)	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	Not Selected	CM-9	CM-9	CM-9
CM-10	Software Usage Restrictions	Not Selected	CM-10	CM-10 (1)	CM-10 (1)
CM-11	User-Installed Software	CM-11	CM-11	CM-11	CM-11 (1)
CP	**Contingency Planning**				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (8)	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Alternate Storage Site	Not Selected	CP-6	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (3)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and	CP-10	CP-10 (2)	CP-10 (2)	CP-10 (2) (4)

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
	Reconstitution				
IA	**Identification and Authentication**				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1)	IA-2 (1) (11)	IA-2 (1) (2) (3) (5) (8) (11) (12)	IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	Not Selected	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4 (4)	IA-4 (4)
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)	IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	Not Selected	Not Selected	IA-8	IA-8 (1) (2) (3) (4)
IR	**Incident Response**				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	IR-3	IR-3	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4	IR-4 (1)	IR-4 (1) (2) (3) (4) (6) (8)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (2)	IR-7 (1) (2)	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	Not Selected	IR-9 (1)	IR-9 (1) (2) (3) (4)	IR-9 (1) (2) (3) (4)
MA	**Maintenance**				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	Not Selected	MA-3 (1)	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
MA-4	Nonlocal Maintenance	MA-4	MA-4	MA-4 (2)	MA-4 (2) (3) (6)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5 (1)	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6	MA-6
MP	**Media Protection**				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2	MP-2
MP-3	Media Marking	Not Selected	MP-3	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6 (1)	MP-6 (1) (2)	MP-6 (1) (2) (3)
MP-7	Media Use	Not Selected	Not Selected	Not Selected	MP-7 (1)
PE	**Physical and Environmental Protection**				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3	PE-3 (1)
PE-4	Access Control For Transmission Medium	Not Selected	PE-4	PE-4	PE-4
PE-5	Access Control For Output Devices	Not Selected	PE-5	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-8	Visitor Access Records	PE-8	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	Not Selected	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	Not Selected	PE-10	PE-10
PE-11	Emergency Power	Not Selected	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	Not Selected	Not Selected	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13	PE-13 (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14 (2)	PE-14 (2)
PE-15	Water Damage Protection	PE-15	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17	PE-17
PE-18	Location of Information	Not Selected	Not Selected	Not Selected	PE-18

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
	System Components				
PL	**Planning**				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2 (3)	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4	PL-4 (1)	PL-4 (1)
PL-8	Information Security Architecture	Not Selected	PL-8	PL-8	PL-8
PS	**Personnel Security (combining HR with IT)**				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	Not Included	Not Included	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3	PS-3 (3)
PS-4	Personnel Termination	PS-4	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8	PS-8
RA	**Risk Assessment**				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3	RA-3
RA-5	Vulnerability Scanning	RA-5 (1) (2)	RA-5 (1) (2)	RA-5 (1) (2) (3) (5) (6) (8)	RA-5 (1) (2) (3) (4) (5) (6) (8) (10)
SA	**System and Services Acquisition**				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3	SA-3
SA-4	Acquisition Process	Not Selected	Not Selected	SA-4 (1)	SA-4 (1) (2) (8) (9) (10)
SA-5	Information System Documentation	SA-5	SA-5	SA-5	SA-5
SA-8	Security Engineering Principles	Not Selected	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9 (1) (2)	SA-9 (1) (2)	SA-9 (1) (2) (4) (5)
SA-10	Developer Configuration	Not Selected	Not Selected	SA-10 (1)	SA-10 (1)

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
	Management				
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11	SA-11 (1) (2) (8)	SA-11 (1) (2) (8)
SA-12	Supply Chain Protection	Not Selected	Not Selected	Not Selected	SA-12
SA-15	Development Process, Standards and Tools	Not Selected	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	Not Selected	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected	Not Selected	SA-17
SC	**System and Communications Protection**				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	Not Selected	SC-3
SC-4	Information In Shared Resources	Not Selected	SC-4	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5	SC-5
SC-6	Resource Availability	Not Selected	Not Selected	SC-6	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (5) (7) (12) (13)	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)	SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8	SC-8 (1)	SC-8 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (2) (3)	SC-12 (1) (2) (3)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices	Not Selected	Not Selected	Not Selected	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17	SC-17
SC-18	Mobile Code	Not Selected	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	Not Selected	SC-19	SC-19

ID	Control Description	Sensitivity Level			
		Low	Low +	Moderate	High (FedRAMP)
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20	SC-20
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name / Address Resolution Service	SC-22	SC-22	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	Not Selected	SC-23	SC-23 (1)
SC-24	Fail in Known State	Not Selected	Not Selected	Not Selected	SC-24
SC-28	Protection of Information At Rest	Not Selected	SC-28	SC-28 (1)	SC-28 (1)
SC-39	Process Isolation	SC-39	SC-39	SC-39	SC-39
SI	**System and Information Integrity**				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2	SI-2 (2) (3)	SI-2 (1) (2) (3)
SI-3	Malicious Code Protection	SI-3	SI-3	SI-3 (1) (2) (7)	SI-3 (1) (2) (7)
SI-4	Information System Monitoring	SI-4	SI-4	SI-4 (1) (2) (4) (5) (14) (16) (23)	SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24)
SI-5	Security Alerts, Advisories and Directives	SI-5	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	Not Selected	Not Selected	SI-6	SI-6
SI-7	Software, Firmware and Information Integrity	Not Selected	SI-7	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1) (2)	SI-8 (1) (2)
SI-10	Information Input Validation	Not Selected	SI-10	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12	SI-12
SI-16	Memory Protection	SI-16	SI-16	SI-16	SI-16