STATERAMP AUTHORIZATION BOUNDARY GUIDANCE

VERSION:
1.0

DATE:
June 2023

DOCUMENT REVISION HISTORY

Date	Description	Version	Governing Body
5/24/2023	Original Publication	1.0	StateRAMP Standards & Technical Committee
6/6/2023	Adopted	1.0	StateRAMP Board of Directors

How to contact us

For questions about StateRAMP, or for technical questions about this document including how to use it, contact *pmo@StateRAMP.org*. For more information about StateRAMP, see www.StateRAMP.org.

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to provide Service Providers (SPs) guidance for developing the authorization boundary for their StateRAMP cloud offering. The authorization boundary provides a diagrammatic illustration that encompasses all technologies, external and internal services, and leveraged systems and users for all State, local or education institution (SLED) data/metadata stored, processed, or transmitted by the cloud service offering.
The information found in this document pertains to SPs that are pursuing and maintaining a StateRAMP Ready, Provisional, or Authorized status.

2. KEY DEFINITIONS AND REQUIREMENTS

2.1 DEFINING THE AUTHORIZATION BOUNDARY

2.1.1 STATERAMP DEFINITION

NIST SP 800-37 defines an authorization boundary as "all components of an information system to be authorized for operation by a sponsor, also known as in-scope components, and excludes separately authorized systems or systems that lack a [StateRAMP] authorization, also known as out-of-scope components, to which the information system is connected."

2.1.2 STATERAMP GUIDANCE

The authorization boundary for cloud technologies must describe a cloud system's internal components and connections to external services and systems that will process SLED data or SLED metadata. All external/3rd party systems and services that process, store, or transmit SLED data/metadata must either be included in the authorization boundary or reside in a StateRAMP authorized system at the same Impact Level (for exceptions refer to Section 2.4.2. Customer-owned systems/services are excluded from the authorization boundary. Service Provider-owned and managed components and technology that are deployed to the customer's environment (i.e. agents, applications, specialized hardware) must be included in the boundary.

When creating the system narratives and descriptions, all data types and dataflows that are depicted in all diagrams within the boundary and all 3rd party and external services/systems that process, transmit or store SLED data and/or metadata, must be included within the narratives and descriptions.

2.2 DATA TYPES

2.2.1 SLED DATA

SLED data is information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for a SLED customer, in any medium or form. SPs must account for, and include within the authorization boundary, all SLED data and/or metadata populated or generated by a SLED customer within the cloud service offering.
Some examples include but are not limited to:

- Mission-based information
- Financial management information
- Human Resources data
- IT management data
- Citizen/taxpayer information

Third-party supplier information

2.2.2 SLED METADATA

NIST SP 800-53 describes metadata as "information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels)." There are two types of metadata that each have their own security considerations and requirements: SLED metadata and corporate metadata. Data that, if compromised, could impact the confidentiality, availability, or integrity of the systems supporting the processing, storage, or transmission of SLED data.

For example:

- Mission-based information types
- Services Delivery Support information types
- Government/State Resource Management information types
- Any other information types as defined in NIST 800-60 Volumes I & II

This is not an exhaustive list and only provides a guideline for determining the impact level of the metadata. If there is a question about the categorization of the metadata in an SP's product, the SP must validate the nature of the metadata with the StateRAMP PMO.
Within the SLED metadata category, there are two subcategories.

SLED metadata with a direct potential impact on mission, organizations or individuals should there be a loss of confidentiality, integrity, or availability. This type of SLED customer metadata must reside within the authorization boundary or within the boundary of another StateRAMP-authorized information system at the same or greater Impact Level.

This includes:

- Security metadata revealing the current security posture of the system
- Vulnerability information
- Active incident response information and communications
- Active threat assessment, penetration test or security investigation information and communications.

SLED metadata with an indirect potential impact on mission, organizations or individuals should there be a loss of confidentiality, integrity, or availability. This type of SLED customer metadata may be

authorized to reside in a system that is fully owned, maintained, and operated by the SP with approval from the StateRAMP PMO.

This includes:

- Data revealing system infrastructure, facilities, and design.
- Application names, versions, and releases
- Application, system, and network configuration information
- Interconnections and access methods
- Systems inventories
- Architecture models, diagrams, and details
- System security plans, contingency plans, risk management plans, security impact analysis, plans, and roadmaps
- Personnel security information: information that could be sold for profit.
- Historical SLED entity metadata that previously was considered to have a direct potential impact.

2.2.3 CORPORATE METADATA

Data about processes within the authorization boundary or SLED customers that does not contain security-sensitive information and/or information that if compromised could be a threat to the systems supporting the processing and storage of SLED data, SLED metadata or SLED personnel data.
For example:

- Sales data
- IT utilization and performance data
- Project planning information
- Marketing materials
- Pricing data

External systems processing or storing corporate metadata can maintain an active connection with the authorization boundary, but all connections must be examined, and the type of information transmitted in the connection must be validated by the 3PAO during initial authorization and during the annual assessment.

2.3 INTERCONNECTIONS

Per NIST SP 800-47, an interconnection is defined as “the direct connection of two or more IT systems for the purpose of sharing data and other information resources.” SPs’ products can utilize external systems, components, and services that are not directly controlled by the SP pursuing a StateRAMP authorization. The SP must clearly document these external services including the flow of the data, specific ports, the security, and encryption used in all the connections and the extent to which SLED data can be impacted using these services. The use of external services that carry SLED data and metadata

must be depicted as part of the authorization boundary and must meet the data requirements for the different data categories. **External systems and services that fall in this category and do not have a StateRAMP authorization must complete a StateRAMP Snapshot and the reliant service provider would be limited to a provisional status until all external systems and services are StateRAMP authorized.** The provisional award letter will include a list of controls and and/or 3rd party systems that must be remediated prior to the award of a full authorization. SP's should make sure their StateRAMP Authorization Package (e.g., System Security Plan [SR-SSP], Security Assessment Plan [SR-SAP], Security Assessment Report [SR-SAR], etc.) reflects this information. As part of issuing the StateRAMP Ready status, the StateRAMP PMO must review and approve the use of the external systems as part of the SP's authorization boundary. As part of issuing the StateRAMP status of Provisional or Authorized, the StateRAMP Approvals Committee (SAC) or the SLED sponsor will also review and approve the use of the external systems as part of the SP's authorization boundary.

2.4 LEVERAGING SERVICES

2.4.1 LEVERAGING EXTERNAL SERVICES WITH A STATERAMP AUTHORIZATION

If a SP's product is leveraging a data subprocessor it must have a StateRAMP status of Authorized or a FedRAMP authorization, and the leveraged SP must demonstrate compliance with all StateRAMP security and privacy requirements. SPs must reflect this relationship within the StateRAMP Security Package and must ensure that they are meeting all the customer requirements outlined in the leveraged customer responsibility matrix.

2.4.2 LEVERAGING EXTERNAL SERVICES WITHOUT A STATERAMP AUTHORIZATION

If a SP's product is leveraging a data subprocessor without a StateRAMP status of Authorized or a FedRAMP authorization, the SP's product is limited to obtaining a Provisional StateRAMP authorization. The leveraged data subprocessor must undergo the StateRAMP Snapshot process and the SP's product would be limited to a provisional status until all external systems and services are StateRAMP authorized. The provisional award letter will include a list of controls and and/or 3rd party systems that must be remediated prior to the award of a full authorization. For the service provider to achieve full authorization the SP's leveraged data sub processor must achieve StateRAMP or FedRAMP authorization, the SP must move the product or service into the authorization boundary, or the SP's product must discontinue use of the unauthorized data subprocessor and move to a product with a current StateRAMP or FedRAMP authorization.

2.4.3 CORPORATE SERVICES

Corporate services are services used by a SP to support their daily business operations. Corporate systems and services exist outside of the authorization boundary and must not contain SLED

data or metadata. Any corporate services that contain SLED metadata must meet the same security requirements that the cloud service offering must meet and be brought into scope of assessment.

2.4.4 ADDITIONAL SLED CUSTOMER-SPECIFIC SECURITY REQUIREMENTS

SLED customers may define additional security requirements in service of the SLED entity's mission and desired security posture. SPs should account for requirements variances on a customer-by-customer basis.

2.5 APPENDIX A: GUIDANCE ON DEVELOPING AUTHORIZATION BOUNDARY, NETWORK AND DATA FLOWS DIAGRAMS

2.5.1 AUTHORIZATION BOUNDARY DIAGRAM (ABD)

Before implementing and documenting security controls, SPs must clearly define the authorization boundary for the product. The authorization boundary is the foundation on which the SR-SSP is built. The authorization boundary is validated against the inventory during the 3PAO assessment.
The Authorization Boundary Diagram (ABD) is a visual representation of the components that make up the authorization boundary and components that are outside of the boundary (external services). The ABD provides the StateRAMP PMO and the SAC or SLED AO with a clear understanding of what is being secured, tested, and authorized.
The ABD is a visual representation of the components that make up the authorization boundary and components that are outside of the boundary (external services).
The following checklist represents StateRAMP's requirements for the ABD and should be used by SPs when developing the ABD:

- Provide an easy-to-read diagram that includes a legend. The ABD should be readable without needing to enlarge it. The ABD can be provided as a separate attachment to the SR-SSP.
- Include a prominent RED border drawn around all components in the authorization boundary.
- Depict all ingress/egress points, IaaS regions, zones, virtual private clouds, subnets, and application and management planes.
- Depict services leveraged from the IaaS/PaaS/SaaS.
- Identify any services that are not StateRAMP authorized.
- Depict all interconnected systems and external services, including corporate services, and identify any systems/services that are not StateRAMP authorized.
    - Depict every tool, service, or component that is mentioned in the SR-SSP narrative and controls.
        - This includes services used to manage and operate the system (e.g., SIEM, vulnerability scanning, system health monitoring, ticketing)
    - Identify all depicted tools, services, or components as either external or internal to the boundary.

    - Depict how SP users and admins and SLED customers access the cloud service (i.e., authentication used to access the service). This will be covered in detail in the Data Flow Diagrams but must be included in the ABD as well.
- If applicable, depict components provided by the SP and installed on customer devices, as inside the authorization boundary. These components should be included in scope for 3PAO testing and included in-boundary.
- Show connections between components within the boundary and to/from external services as well as the separation and security in-place between the boundary and external services and access.
- Depict dev/test environment, alternate processing site, and location of backups including the connections and security mechanisms associated with the connections and services.
    - The dev/test environment must be included within the boundary if SLED data is used and/or if SLED personnel have access to the environment for any reason, including training and user acceptance testing.
- Show update services (e.g., malware signatures and OS updates) outside the boundary.

The ABD should also depict:

- External systems/services that provide functionality to the product or are used to manage and operate the product. This includes underlying IaaS/PaaS/SaaS offerings, system interconnections, APIs, external cloud services, and corporate shared services.
- System components, services, or devices that reside in the customer's environment may be in boundary, or out.
    - For example, many SPs require customers to authenticate via an IdP. This should be depicted as out-of-boundary on the ABD.

2.5.2 NETWORK DIAGRAM

The Network Diagram should address all components reflected in the ABD, and:

- Depict subnetting
- Depict location of DNS servers including:
    - External authoritative servers used by customers to access the CSO
    - Internal recursive servers used to access domains outside the boundary

2.5.3 DATA FLOW DIAGRAMS (DFDS)

The Data Flow Diagrams should address all components reflected in the ABD. At a minimum, SR-SSPs should include diagrams for the following logical data flows:

- SLED customer user and SLED customer admin authentication, including type of Multifactor Authentication (MFA)
- SP administrative and support personnel authentication, including type of MFA
- System application data flow within the Authorization Boundary
- System application data flow to/from:
    - External services, including corporate shared services

- Interconnected systems
- Alternate processing sites and backup storage
- Dev/Test environment

Each DFD should explicitly identify:

- Everywhere (internal & external) SLED data and metadata at rest and in transit is not protected through encryption
- Everywhere SLED data is protected through encryption

Common quality issues for data flow diagrams include:

- Does not depict all access by all parties (e.g., SP admins, SLED customers, IaaS/PaaS portal)
- Does not indicate MFA tool and protocol (OTP, push, etc.) employed for administrative/support personnel and SLED customers
- Lacks port and protocol information
- Does not indicate encryption of data in transit and data at rest
- Fails to include internal flows such as to data stores, or within a microservices environment
- Fails to address replication of data to alternate processing site, or to backup storage
- Does not include a legend

2.6 APPENDIX B: FREQUENTLY ASKED QUESTIONS

2.6.1 WHAT IS AN AUTHORIZATION BOUNDARY AND WHY IS IT IMPORTANT?

The authorization boundary is the foundation on which the system security plan is built. The term "authorization boundary" exclusively refers to the technology (hardware, software), physical or virtual, that comprises the system to be authorized for use for SLED entities by the StateRAMP PMO comprising the system to be authorized for operation or authorized for use by the StateRAMP PMO, the SAC or the SLED AO.

Before implementing and documenting security controls, SPs must clearly define the authorization boundary for the product. The Authorization Boundary Diagram (ABD) is a visual representation of the components that make up the authorization boundary and components that are outside of the boundary (external services). The ABD provides the StateRAMP PMO and the SAC or the SLED AO with a clear understanding of what is being secured, tested, and authorized.

Refer to Appendix A for a list of requirements for the ABD.

2.6.2 DOES A SYSTEM THAT STORES OR PROCESSES SLED DATA/METADATA OR SENSITIVE SYSTEM DATA, BUT IS NOT DIRECTLY CONNECTED TO THE BOUNDARY, NEED TO BE IDENTIFIED AS AN EXTERNAL SYSTEM AND/OR SERVICE?

Yes. The authorization boundary diagram and description must include any external system or service that contains SLED data/metadata or sensitive data about the SP's product. In addition, every tool, service, or component that is mentioned in the SR-SSP and excluded from testing should be evaluated as an external service. For example, an external ticketing system that is used to capture and track system vulnerabilities may not be directly connected to the SP's product, but still contains sensitive data that could impact the confidentiality, integrity or availability of the product. These types of external systems and services must be depicted on the ABD and described in the authorization package deliverables (SR-SSP, SR-SAP, SR-SAR and all applicable security documentation) or Readiness Assessment Report (for SPs pursuing a StateRAMP Ready status).

2.6.3 HOW DOES STATERAMP DEFINE "CORPORATE" SERVICES?

Corporate services are services in the SP corporate environment that are used to manage parts of the system. Systems that are in the SPs corporate environment that do not process, transmit, or store SLED information do not have to meet the requirements of the StateRAMP baselines. However, they must be included on the authorization boundary diagram and data flow diagram and the narrative must explicitly state what is being used, why it is being used, what data it is collecting, and how SLED data is protected using this corporate component/system. If any systems in the SP corporate environment process, transmit, or store any SLED data, the system is considered in scope and must be included in the authorization boundary as a component seeking SR authorization and it must meet the requirements of the SR baselines. Corporate services that support a StateRAMP boundary environment must be depicted on the ABD and DFDs and described in the SR-SSP as external systems or services, and risks associated with connections to corporate systems or services should likewise be described in 3PAO assessment results (SR-SAR or SR-RAR).