STATERAMP INCIDENT COMMUNICATIONS PROCEDURES

VERSION:
1.0

DATE:
August 2022

Contents

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
7/22/2022	Policy Approved	1.0	Standards & Technical Committee
8/7/2022	Policy Adopted	1.0	Board of Directors

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

1. INTRODUCTION AND PURPOSE

This document describes the process for StateRAMP stakeholders to use when reporting information concerning information system security incidents or suspected information system security incidents. In addition, this document outlines the responsibilities of all StateRAMP stakeholders and provides a sequence of required communications that ensure accurate and timely information is reported to all relevant stakeholders.

StateRAMP Stakeholders include:

- Service providers (SP)
- StateRAMP Program Management Office (PMO)
- StateRAMP Approvals Committee (SAC)
- US-CERT
- SP customers
- SP-relying parties (including leveraging SPs)
- Interconnected system owners

This document will adhere to the definition of an incident as described by the Federal Information Security Modernization Act of 2014 (FISMA). FISMA defines an incident as an occurrence that:

a. actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

b. constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

After an SP obtains a Ready or Authorized status for its service offering, it enters the continuous monitoring (ConMon) phase of the NIST Risk Management Framework (RMF). A critical element of ConMon is timely and clear communications regarding any actual or suspected incidents. Such communications ensure that incident handling is transparent and keeps all stakeholders aware of the incident's status and the status of any remediation efforts.

SPs with a Ready or Authorized status are required to report any incident, whether confirmed or suspected, that results in the loss, or potential loss, of confidentiality, integrity, or availability of the cloud service or the data and/or metadata that the service stores, processes or transmits so that affected entities can take steps to protect data and ensure a resolution is reached in a timely manner.

Reporting incidents to StateRAMP stakeholders does not result in punitive actions against the SP. However, failure to report incidents will result in escalation actions against the SP as defined in the StateRAMP Continuous Monitoring Performance Guidance.

1.1 COMPLIANCE

The StateRAMP Continuous Monitoring Performance Guidance defines the requirements for ConMon performance. It explains the actions StateRAMP will take when an SP fails to maintain an adequate

continuous monitoring strategy. This includes issues related to and communication of information security incidents.

Failure of an SP to report an incident or suspected incident according to the procedures laid out in this document will result in the issuance of a Corrective Action Plan (CAP). A second violation of an SP to report an incident or suspected incident according to these communication procedures may result in the revocation of the SP's Ready or Authorized status.

1.2 APPLICABLE STANDARDS AND GUIDANCE

The following standards and guidance are helpful for understanding incident communication planning:

- Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 2]
- Managing Security Information Risk [NIST SP 800-39]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30, Revision 1]
- CISA Incident Reporting Guidelines
- US-CERT Federal Incident Notification Guidelines

1.3 ASSUMPTIONS

Assumptions used in this document are as follows:

- Key SP personnel have been identified and are trained in their relevant incident roles and responsibilities.
- Government sponsor Incident Response Plans are in place.
- SP Incident Response Plans are in place and have been tested in accordance with StateRAMP IR controls.
- Both internal and external incident response contact lists in all Incident Response Plans are accurate and up to date.
- All contact information for StateRAMP SPs must be kept up to date and on file with the StateRAMP PMO as well as all registered government sponsors of an SP's StateRAMP Ready or Authorized services. For the StateRAMP PMO, email pmo@stateramp.org.

1.4 ROLES & RESPONSIBILITIES

1.4.1 CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

The Cybersecurity & Infrastructure Security Agency (CISA) serves as a risk advisor for state, local, tribal, and territorial governments, academia, and private businesses. CISA offers a range of resources available at https://www.cisa.gov/uscert/resources.

1.4.2 UNITED STATES COMPUTER EMERGENCY READINESS TEAM

The United States Computer Emergency Readiness Team (US-CERT) provides incident handling assistance, as needed, to SPs and sponsoring governments.

1.4.3 STATERAMP PMO

The StateRAMP PMO coordinates signature and approval of Corrective Action Plan (CAP), suspensions, and revocations, including those related to information security incidents with the StateRAMP Approvals Committee or the SLED Authorizing Official**.** The PMO will monitor an SP's compliance with the *StateRAMP Continuous Monitoring Performance Guidance.* The PMO will provide guidance and oversight related to incidents and make risk-based recommendations to the StateRAMP Approvals Committee (SAC) or the sponsoring government's Authorizing Official (AO). The PMO will confirm with the SP that the SP has reported the incident to US-CERT, has obtained a US-CERT tracking number, has communicated the incident to its customers, and is following its IR Plan. The PMO also has the ability to suspend or revoke a system's Ready authorization should the SP fail to adhere to StateRAMP guidelines for incident reporting.

1.4.4 STATERAMP APPROVALS COMMITTEE

The StateRAMP Approvals Committee (SAC) authorizes systems on a case-by-case basis after a thorough evaluation of the system through the SAC authorization process. The SAC coordinates with the PMO to monitor a system's security status and can suspend or revoke an Authorized status granted by the SAC should the SP fail to adhere to StateRAMP guidelines for incident reporting.

1.4.5 AUTHORIZING OFFICIAL

The Authorizing Official (AO) is the individual acting on behalf of the sponsoring government that grants an SP an Authorized or Provisional status. The AO, on behalf of the government sponsor, notifies the SP, US-CERT, and the StateRAMP PMO if the government sponsor becomes aware of an incident or suspected incident that an SP has not yet reported. The AO ensures that requirements for sponsor-specific Incident Response (IR) plans are met. The AO also confirms with the SP that the SP has reported the incident to US-CERT and has obtained its US-CERT tracking number for those systems authorized by the AO.

1.4.6 SERVICE PROVIDER

The SP is responsible for protecting incident information commensurate with the impact level of the service offering. The SP must maintain a satisfactory risk management program for the cloud service in accordance with StateRAMP guidelines and comply with all IR guidance and requirements. The SP must maintain a list of all current customers and the proper communication channels with all StateRAMP POCs and 3PAOs.

The SP notifies affected SLED customers of information security incidents. The SP notifies US-CERT of information security as needed and provides the US-CERT tracking number to the StateRAMP PMO at pmo-stateramp@knowledgeservices.com, as well as all applicable stakeholders of information security incidents, and provides status updates thereafter. The SP requests assistance from US-CERT as needed.

Finally, the SP provides a final report to StateRAMP PMO at pmo-stateramp@knowledgeservices.com as well as applicable stakeholders to include the sponsoring AO or SAC representatives after completion of the Post-Incident Activity phase of the Incident Response Life Cycle as described in NIST SP 800-61 rev2, *Computer Incident Handling Guide*.

1.4.7 THIRD PARTY ASSESSMENT ORGANIZATION

The Third Party Assessment Organization (3PAO) performs any required independent security assessment related to information security incidents.

2. GENERAL PROVIDER REPORTING PROCESS

SPs must report all incidents, whether suspected or confirmed events, that result in the potential or confirmed loss of confidentiality, integrity, or availability to assets or services provided by the authorization boundary. Reporting requirements to US-CERT, government sponsors of the cloud service offering, and StateRAMP POCs are identified in this section.

As SPs manage and report incidents, they must adhere to the StateRAMP requirements in protecting the system's data and/or metadata as well as any data about the system and data related to events. Sensitive information must be provided using the StateRAMP PMO repository. Additional notifications may be sent to PMO@StateRAMP.org. **SPs must report suspected and confirmed information security incidents within one hour of identification by the SP's IR team, Security Operations Center (SOC), or information technology department to the following parties:**

- Government sponsors and registered government clients who are impacted or suspected of being impacted
- US-CERT (https://us-cert.cisa.gov/forms/report)
- StateRAMP PMO

US-CERT may take up to one hour to provide a tracking number, and the SP must provide the tracking number to the StateRAMP PMO as soon as it is made available by US-CERT. Incident notifications provided by the SP to any POCs verbally (e.g., by phone) must be followed up in writing. However, sensitive information must be protected (e.g., by encrypted email or the StateRAMP PMO's secure document repository).

When reporting to US-CERT, SPs must include the required data elements, as well as any other available information. SPs must submit incident notifications in accordance with the Submitting Incident notifications section of https://www.us-cert.gov/incident-notification-guidelines.

After initial incident notification, the SP must provide updates to US-CERT as agreed to, as well as daily updates to the StateRAMP PMO. The final daily update must be provided to the StateRAMP PMO after the SP has completed the Recovery phase of the Incident Response Life Cycle. The SP must also provide a report to the StateRAMP PMO after the SP has completed the Post-Incident Activity in the Incident Response Life Cycle. The final report must describe what occurred, the root cause, the SP's response, lessons learned, and changes needed.

SPs are responsible for responding to emergency inquiries from StateRAMP. If any emergency inquiry is issued, the SP must comply with the request's timeline. If there are any explicit actions the SP must take that are identified in the emergency inquiry, they must be addressed in the timeline prescribed. Failure to report or respond to emergency inquiries, or failure to perform the prescribed remediation actions, can result in the escalation actions outlined in the Continuous Monitoring Performance Guidance.

The StateRAMP PMO, in coordination with the AO or SAC, will evaluate the final report submitted by the SP and determine an appropriate path forward. This may include developing Plans of Action and Milestones (POA&M) and/or CAPs to address areas needing improvement.