FedRAMP

FedRAMP Incident Communications Procedures

Version 4.0

04/15/2021

GSA

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
04/02/2013	1.0	All	Initial FedRAMP Incident Communication Procedure	FedRAMP PMO
06/06/2017	2.0	All	Updated logo	FedRAMP PMO
12/08/2017	3.0	All	Updated to newest template	FedRAMP PMO
04/15/2021	4.0	All	Updated to align with revised guidance from US-CERT. and Incorporated new formatting, incident explanation, and compliance requirements.	FedRAMP PMO

TABLE OF CONTENTS

Introduction and Purpose

Information systems are vital to a federal agency's mission and business functions. Therefore, it is absolutely critical that services provided to agencies operate effectively without interruptions. This *Incident Communications Procedures document* outlines the steps for FedRAMP stakeholders to use when reporting information concerning information security incidents, including response to published Emergency Directives. The steps included in this document provide a sequence of required communications that are in place to ensure accurate and timely information is reported to all relevant stakeholders.

FedRAMP stakeholders include a variety of teams and individuals with a vested interest in the successful implementation and operations of FedRAMP. They include:

- Cloud Service Providers (CSPs)
- FedRAMP Joint Authorization Board (JAB)
- FedRAMP Program Management Office (PMO)
- US-Computer Emergency Readiness Team (US-CERT)
- CSP customers (including federal agencies and other FedRAMP-approved CSPs)
- CSP-relying parties (Including leveraging CSPs)
- Interconnected Systems.

The Federal Information Security Modernization Act of 2014 (FISMA)[1] is the authoritative source for incident definitions. 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." The terms "security incident" and "information security incident" are also used interchangeably with "incident" within the body of the law.

After a CSP obtains a FedRAMP Agency Authorization To Operate (ATO) or Provisional-AuthorizationTo Operate (P-ATO) for its service offering, it enters the continuous monitoring (ConMon) phase. Clear and timely incident communication to relevant stakeholders is a *key* aspect of ConMon to ensure that all incident handling is transparent, and so that all stakeholders are aware of the current status and remediation efforts.

FedRAMP requires CSPs to report any incident (suspected or confirmed) that results in the actual or potential loss of confidentiality, integrity, or availability of the cloud service or the data/metadata that it stores, processes, or transmits. Reporting real and suspected incidents allows agencies and other affected customers to take steps to protect important data, to maintain a normal level of efficiency, and to ensure a full resolution is achieved in a timely manner.[2]

Reporting incidents or suspected incidents, as well as responses to Emergency Directives to the appropriate FedRAMP stakeholders does not result in punitive actions against the CSP. However, failure to report incidents will result in escalation actions against a CSP as defined in the Continuous Monitoring Performance Management Guide. A collaborative approach to reporting incidents between CSPs and the FedRAMP

[1] See 44 U.S.C. § 3552(b)(2)

[2] FedRAMP complies with NIST standards and guidance. With respect to incidents, it follows NIST Special Publication 800-61, Revision 2, CISA guidance and the US-CERT Federal Incident Notifications Guidelines. In accordance with these standards and guidance, additional program-specific guidance and procedures are provided in this document to aid all stakeholders with respect to reporting incidents.

stakeholders allows all parties to be aware of and successfully manage the risk associated with an incident and to classify and resolve suspected incidents.

Applicability

The information found in this document pertains to CSPs that have been issued a FedRAMP P-ATO and/or an Agency ATO.

Compliance

The *Continuous Monitoring Performance Management Guide* defines requirements for Continuous Monitoring Performance Management. It explains the actions FedRAMP will take when a CSP fails to maintain an adequate risk management program, including issues related to and communication of information security incidents.

Failure of a CSP to report an incident or suspected incident according to these communication procedures will result in the issuance of a Corrective Action Plan (CAP). A second violation of a CSP to report an incident or suspected incident according to these communication procedures may result in the suspension of the CSP's ATO or P-ATO.

Applicable Laws and Regulations

The following laws and regulations are applicable to incident planning:

- Federal Information Security Modernization Act (FISMA) of 2014
- Management of Federal Information Resources [OMB Circular A-130]
- Records Management by Federal Agencies [44 USC 31]
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information [OMB Memo M-07-16]

Applicable Standards and Guidance

The following standards and guidance are useful 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

Assumptions

Assumptions used in this document are as follows:

- Key CSP personnel have been identified and are trained in their relevant incident roles and responsibilities.
- Agency *Incident Response Plans* are in place.
- CSP *Incident Response Plans* are in place and have been tested in accordance with FedRAMP 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 FedRAMP CSPs must be kept up to date and on file with the FedRAMP PMO, JAB, and all federal customers of a CSP's FedRAMP Authorized services. For the PMO, email fedramp_security@gsa.gov and for the JAB, email your JAB reviewers.

Roles and Responsibilities

The following table outlines the roles and responsibilities for the various stakeholders in the incident communication process.

	Role	Responsibility
CISA	Risk Advisor	• Coordinates security and resilience efforts across private and public sectors • Delivers technical assistance and assessments to federal stakeholders and infrastructure owners nationwide • Conducts nationwide outreach to support and promote the ability of emergency response providers and relevant government officials in the event of an emergency
US-CERT	Incident Handling	• Provides incident handling assistance, as needed, to CSPs and Agencies

		• Provides reporting for any identified incidents affecting government or government contracted systems to appropriate stakeholders
FedRAMP PMO	Monitors Incident Communication Process	• Coordinates signature and approval of Corrective Action Plan (CAP), Suspensions, and Revocations including those related to information security incidents with the JAB Technical Representatives Principles (TRs) • Monitors Performance Management Plan • Acts as the primary ConMon process interface between the JAB and the PMO and provides recommendations and status updates, including those for incidents, to the FedRAMP Director • Supports and advises JAB Reviewers as needed
Agency	Agency Authorizing Official (AO)	• Acts as final approval authority for the use of a system by their agency • Notifies CSP, US-CERT and FedRAMP stakeholders if the agency becomes aware of an incident or suspected that a CSP has not yet reported • Ensures requirements for agency-specific Incident Response (IR) plans are met • For Agency Authorizations, confirms with CSP that the CSP has reported the incident to US-CERT and has obtained its US-CERT tracking number
JAB Team	Joint Authorization Board (JAB)	• Composed of the CIOs of the Department of Defense (DOD), General Services Administration (GSA), and Department of Homeland Security (DHS) • Authorizes, denies, monitors, suspends, and revokes a CSP's P-ATO and JAB P-ATO as appropriate • Reviews, approves, and signs CAPs being issued to CSPs
	JAB Technical Representative (TR) Principal	Composed of one Principal Technical Reviewer from DOD, GSA, and DHS • Provides guidance and oversight related to information security incidents • Effects policy change relating to information security incidents
	JAB Reviewer Team Lead	• One of three JAB Reviewer Team Leads., One from DOD, GSA, and DHS • Makes risk-based recommendations to JAB TR Principal, related to information security incidents • Advises JAB Reviewers and provides general oversight of all ConMon process areas, including those related to information security incidents

	JAB Reviewers	• A team of three JAB Reviewers, with one from the DOD, GSA, and DHS • Serves as primary interface for ConMon activities, including reviewing information security incidents, between JAB TR Principals, FedRAMP PMO, CSP, and 3PAO for JAB Authorized systems • Distributes incident notifications, information, risk-based recommendations, and other status updates to other JAB Reviewers, JAB TR leads and FedRAMP PMO in a secure manner • Confirms with CSP that the CSP has reported the incident to US-CERT, has obtained its US-CERT tracking number, has communicated the incident to its customers, and is following its IR Plan
CSP/3PAO	Cloud Service Provider (CSP)	• Protects incident information commensurate with the impact-level of the cloud service • Maintains a satisfactory Risk Management Program for the cloud service in accordance with FedRAMP guidelines • Complies with IR guidance and requirements • Maintains a list of all current customers and the proper communication channels with all AOs and 3PAOs • Notifies affected customers of information security incidents • Notifies US-CERT of information security incidents, as needed (see CSP General Reporting Process section), and provides the US-CERT tracking number to FedRAMP PMO at fedramp_security@gsa.gov as well as all applicable stakeholders of information security incidents, and provides status updates thereafter • Requests assistance from US-CERT as needed • Provides a final report to FedRAMP PMO at fedramp_security@gsa.gov as well as applicable stakeholders to include the agency AO or JAB representatives after completion of the Post-Incident Activity phase of the Incident Response Life Cycle[3]
	Third Party Assessment Organization (3PAO)	• Performs any required independent security assessment related to information security incidents

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Revision 2, Computer Incident Handling Guide*

CSP General Reporting Process

CSPs must report all incidents, which include any suspected or confirmed event, that results 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, agency customers of the cloud service offering, and FedRAMP POCs are identified in this section (see Appendix A for a graphical representation of the steps outlined in this section).[4]

As CSPs manage and report incidents, they must not deviate from FedRAMP requirements to protect the confidentiality, integrity, or availability of data/metadata stored, processed, or transmitted by the system as well as data about the system and related to the incident. Sensitive information must be provided using approved mechanisms. CSPs must report suspected, and confirmed information security incidents to the following parties **within one hour** of being identified by the CSP's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department:

- Customers who are impacted or who are suspected of being impacted (via the CSP Incident Response folder in their respective FedRAMP secure repository)
- US-CERT, under the following conditions: The CSP has confirmed, has yet to confirm, or suspects the incident is the result of any of the attack vectors listed in https://www.us-cert.gov/incident-notification-guidelines#attack-vectors-taxonomy.
    - Reporting Location: https://us-cert.cisa.gov/forms/report
- FedRAMP POCs
    - Agency POCs
        - Agency AOs
        - Agency Incident Response Teams (as identified by the authorizing agency)
    - JAB POCs *(only applicable for JAB Authorized)*
        - JAB Reviewers (contact information on file with the CSP)
        - JAB Reviewer Team Leads (contact information on file with the CSP)
        - PMO at fedramp_security@gsa.gov

FedRAMP encourages the use of automated mechanisms for incident reporting. If a CSP wants to leverage automated incident reporting mechanisms the CSP must work with the FedRAMP POCs and AOs to ensure the content and context of the automated reporting provides the required information.

CSPs must maintain current and accurate contact information on file for FedRAMP POCs. Since US-CERT may take up to one hour to provide a tracking number, the CSP must provide the tracking number to FedRAMP POCs as soon as it is made available by US-CERT. Incident notifications provided by the CSP to any FedRAMP POCs verbally (e.g., by phone) must be followed up by an email. However, sensitive information must be protected.

When reporting to US-CERT, CSPs must include the required data elements, as well as any other available information. CSPs must submit incident notifications in accordance with the Submitting Incident Notifications section of https://www.us-cert.gov/incident-notification-guidelines. In some cases, it may not be feasible to

[4] US-CERT Federal Incident Notification Guidance, https://us-cert.cisa.gov/incident-notification-guidelines

have complete and validated information prior to reporting. CSPs should provide their best estimate at the time of notification and report updated information as it becomes available.

After initial incident notification, the CSP must provide updates to US-CERT as agreed to as well as daily updates to the FedRAMP POCs. The final daily update must be provided to FedRAMP POCs after the CSP has completed the Recovery phase of Incident Response Life Cycle (Containment, Eradication, Recovery and Post-Incident Activity). The CSP must also provide a report to the FedRAMP POCs after it has completed the Post-Incident Activity in the Incident Response Life Cycle[5]. The final report must describe what occurred, the root cause, the CSP's response, lessons learned, and changes needed.

Additionally, CSPs are responsible for responding to emergency inquiries from FedRAMP, including those that are the result of the issuance of CISA Emergency Directives. If any emergency inquiry is issued, the CSP must comply within the timeline described in the request. Any additional reporting requirements identified in the inquiry must also be met. Relatedly, if there are any explicit actions the CSP 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 Guide.

JAB Reviewers' Responsibilities

Upon receipt of the CSP's notification, the JAB Reviewers must take the following actions:

1. Verify that customers who are impacted and suspected of being impacted have been notified.
2. Verify that, if required (see section 3), US-CERT has been notified.
3. Request that the CSP provides daily updates and the US-CERT tracking number when it has become available.
4. Verify the CSP's notification and supporting documentation is posted to the secure reporting repository and notifications. Notifications of incidents should be sent to the following FedRAMP POCs after each update, should not contain any sensitive data, and direct POCs to the secure repository:
    a. FedRAMP PMO at fedramp_security@gsa.gov
    b. JAB Reviewers (contact information on file with the CSP)
    c. JAB Reviewer Team Leads (contact information on file with the CSP)
5. Ensure information related to the incident is in the CSP's designated secure file repository.

JAB Reviewers, in coordination with the JAB Reviewer Team Leads and JAB TRs, will evaluate the final report, submitted by the CSP, and determine an appropriate path forward. This may include developing Plans of Action and Milestones (POA&Ms) and/or CAPs to address areas needing improvement.

[5] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Revision 2, Computer Incident Handling Guide*

Appendix A: CSP General Reporting Process Graphic

The below diagram provides a high-level overview of the steps a CSP should take if a security incident occurs. For more specific information about the stakeholders referenced below, please see page 6.