FedRAMP INCIDENT COMMUNICATION PROCEDURE

Version 3.0

December 8, 2017

FedRAMP

EXECUTIVE SUMMARY

This document supports the Incident Communication Procedure for the Federal Risk and Authorization Management Program (FedRAMP). This Incident Communication Procedure outlines the measures to consider in order for all parties to effectively communicate during a security incident incurred by a FedRAMP authorized cloud service provider. The measures described herein include how the FedRAMP Information System Security Officer (ISSO) manages the incident communication process, and identifies who the Cloud Service Providers and federal departments and agencies should call to report an incident, when to contact the United States Computer Emergency Readiness Team (US-CERT) for assistance, and how to ensure that all incidents are communicated to the stakeholders.

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

ABOUT THIS DOCUMENT

This document has been developed to provide guidance and procedures for FedRAMP security incident communications.

WHO SHOULD USE THIS DOCUMENT?

The audience of this document is FedRAMP ISSOs, Cloud Service Providers, US-CERT, and federal agencies.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into six sections. Some sections include subsections.

Section 1 describes the introduction and provides an overview and includes the purpose of the document as well as the authorities and standards.

Section 2 describes the incident communication objectives.

Section 3 describes the incident communications roles and responsibilities.

Section 4 describes the stakeholder communication flow process. The communication flow is described to ensure that all appropriate personnel are aware of an incident.

Section 5 describes the life-cycle of a security incident, and what stakeholders should consider to respond effectively.

Appendix A describes example incident communications scenarios.

CONVENTIONS USED IN THIS DOCUMENT

This document uses the following typographical conventions:

Italic

Italics are used for email addresses, security control assignments parameters, and formal document names.

Italic blue in a box

Italic blue text in a blue box indicates instructions to the individual filling out the template.

Example Instruction: This is an instruction to the individual filling out of the template

Bold

Bold text indicates a parameter or an additional requirement.

Notes

Notes are found between parallel lines and include additional information that may be helpful to the users of this document.

Example Note: *This is a note.*

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION AND PURPOSE

Information systems are vital to a federal agency's mission/business functions; therefore, it is critical that services provided to agencies operate effectively without interruptions. This *Incident Communication Procedure* outlines the steps for FedRAMP stakeholders to use when communicating information related to security incidents. The steps include the sequence of communications that should take place to ensure that all necessary information is communicated from one stakeholder to other stakeholders.

FedRAMP stakeholders are those individuals and teams with a vested interest in the successful implementation and operations of FedRAMP. Therefore, FedRAMP stakeholders include:

- CSPs
- FedRAMP ISSOs
- FedRAMP PMO
- US-CERT
- Customer agencies

The nature of unprecedented disruptions can create confusion, and often predisposes an otherwise competent IT staff towards less efficient practices. To maintain a normal level of efficiency, it is important to decrease the real-time process engineering by documenting the incident communication process prior to the occurrence of an incident.

It is the goal of this *Incident Communication Procedure* to assist CSPs and federal agencies to ensure all appropriate stakeholders are informed of the current status of incidents, so that a full resolution is achieved in a timely manner.

1.1. APPLICABILITY

The information found in this document pertains only to Cloud Service Providers (CSPs) that have been issued a Provisional Authorization through the FedRAMP Joint Authorization Board (JAB). Other CSPs that have been issued government Authorizations to Operate (ATOs) should follow their own respective *Incident Response Plans* that have been previously assessed and authorized by their agency customers.

1.2. APPLICABLE LAWS AND REGULATIONS

The following laws and regulations are applicable to incident planning:

- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- 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]

1.3. 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 1]
- 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]

1.4. ASSUMPTIONS

Assumptions used in this document are as follows:

- Key personnel have been identified and are trained in their roles
- Key personnel have access to this *Incident Communication Procedure*
- US-CERT is available 24 x 7 x 365
- The affected agency has access to the contact information for all responsible parties
- Agency *Incident Response Plans* are in place and have been tested
- CSP *Incident Response Plans* are in place and have been tested
- CSPs have contractual language in place to allow sharing of relevant incident data
- Contact lists in all *Incident Response Plans* are accurate and up to date
- Stakeholder contact lists have been distributed to all stakeholders.

2. OBJECTIVE

The primary objective of this document is to ensure all stakeholders communicate with each other whenever an incident occurs, allowing for a team-based approach so that incidents can be resolved quickly. Collaboration among stakeholders often results in faster resolution of the incident.

3. ROLES AND RESPONSIBILITIES

The FedRAMP ISSO has oversight responsibility for ensuring appropriate communications occurs for all reported outages, disruptions, and incidents for CSP systems with a FedRAMP JAB Provisional Authorization. FedRAMP ISSOs are trained in their duties, and ensure all appropriate parties are made aware of the status of incidents.

The shared tenant architecture of cloud services implies that a single incident may impact multiple federal agencies leveraging the same cloud services. FedRAMP requires CSPs to report all incidents. Incident reporting responsibilities are discussed in the subsequent sections of this document.

All incidents have the notion of *first response*. A *first responder* is the individual who first brings the incident (or suspected incident) to the attention of others. A first responder can be any type of user (e.g. a system administrator, a customer) or a monitoring center. In the case of FedRAMP, a first responder could be a CSP, an agency customer, or US-CERT.

Note: *The US-CERT website can be found at the following URL:* http://www.us-cert.gov

Working as a team, agencies, FedRAMP ISSOs, CSPs, and the US-CERT are positioned to handle and resolve incidents faster through collaborative methods than if each entity worked on the incidents alone.

> FISMA §3546 requires that US-CERT:
>
> *Provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents.*

If CSPs require additional assistance in incident resolution, they will need to communicate this need to US-CERT. CSPs should have the understanding that asking for additional incident support, and resolving the incident quickly, will have fewer repercussions on customers systems, and on their Provisional Authorization, than refusing assistance and leaving the incident unresolved for a much longer period of time. FedRAMP recognizes that CSPs have their own incident response capabilities and asking for assistance is entirely optional, though incident reporting is mandatory. CSPs should make a judgment call on when to ask for outside assistance based on their own capabilities and the factors surrounding each unique incident.

The following sections outline the roles and responsibilities for the various stakeholders in the incident communication process.

3.1. FEDRAMP ISSO

All CSPs that have obtained a FedRAMP Provisional Authorization are assigned a FedRAMP ISSO by the FedRAMP Program Management Office (PMO). FedRAMP ISSOs are headquartered at the Office of the FedRAMP PMO. Supporting the PMO, FedRAMP ISSOs provide overight for CSP security incidents. OMB Circular A-130 §(8)(b)(1)(b)xi requires that federal agencies:

> *Establish oversight mechanisms to evaluate systematically and ensure the continuing security, interoperability, and availability of systems and their data.*

FedRAMP ISSOs are not first responders and are dependent on after action reports from other stakeholders. The role of FedRAMP ISSOs in the incident communication process is described below.

- Receives notification of incident from first responders
- Confirms with CSP that CSP is following their *Incident Response Plan*
- Records all incident communications in the FedRAMP database

- Ensures that the appropriate stakeholders are kept updated
- Monitors the communication flow between stakeholders
- Ensures timely closure of all incidents
- Ensures that POA&Ms are created if needed as a result of an incident
- Discusses with CSP the option of requesting outside assistance (e.g. US-CERT)
- Makes use of after action reports to facilitate further communications
- In the event of a major incident affecting multiple agencies, escalates and facilitates communications to FedRAMP Director and Joint Authorization Board and others as necessary.

Note: *At this time, FedRAMP ISSOs are available during regular business hours, Eastern time. CSPs requiring assistance off hours and during federal holidays should contact US-CERT.*

3.2. CLOUD SERVICE PROVIDER

Whenever a CSP detects an incident, it should be reported to all affected customer agencies based on the categorization of the incident. The CSP should also inform the affected agencies POCs whenever US-CERT assistance is required. CSP general responsibilities are described below.

- For incidents related to unauthorized access or personally identifiable information, report the incident to US-CERT within one hour of awareness (required by OMB Memo M-07-16).
- Notifications should be done via telephone and followed up with an email
- Use phone numbers and email addresses as provided by the FedRAMP PMO
- If necessary, request assistance from the US-CERT
- Follow procedures in the system *Incident Response Plan*
- Log all incident details on Incident Reporting Form (found in *Incident Response Plan*)
- Follow the *Configuration Management Plan* for change control
- Manage and maintain a Continuous Monitoring program
- As required by the *FedRAMP Continuous Monitoring Guide and Strategy*, report incidents as they occur and annually through the Self-Attestation template.

Note: *The OMB memo (M-07-16) that references the OMB one hour rule can be found at the following URL: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf*

3.3. FEDERAL AGENCY

Agencies should report all incidents consistent with the agency's incident response policy. Each agency should designate a primary and secondary POC for incident communications. Agency POCs should be shared with the FedRAMP ISSO team, US-CERT, and all CSPs (under contract with the agency). When CSPs report incidents to agencies, agencies should in every case offer to coordinate assistance between US-CERT and the CSPs. Agency general responsibilities are described below.

- Notify CSP if the agency becomes aware of an incident that a CSP has not yet reported
- Provide a primary and secondary POC for CSPs and US-CERT as described in agency and CSP *Incident Response Plans*
- Notify US-CERT when a CSP reports an incident
- Work with CSPs to resolve incidents; provide coordination with US-CERT if necessary
- Notify FedRAMP ISSO of CSP incident activity
- Monitor security controls that are agency responsibilities.

3.4. US-CERT

FISMA requires federal agencies to report incidents US-CERT acts as the government wide incident response organization that assists civilian federal agencies in their incident handling efforts. US-CERT does not replace any existing agency response teams; rather, it augments the efforts of the federal civilian agencies by serving as a focal point when dealing with incidents. The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546 and are summarized as follows:

- Notify agency POCs, CSPs, and FedRAMP ISSOs of known incidents
- Coordinate cyber security operations and incident response
- Monitor and report security incidents and network flow data
- Distribute advisories on potential threats
- Assists government-wide and agency-specific efforts to provide adequate, risk- based and cost-effective cyber security.

Separate procedures are in place for the Department of Defense as identified in Directive O-8530-1 and all components report incidents to the Joint Task Force Global Network Operations (JTF-GNO), which, in turn, coordinates directly with the US-CERT.

4. STAKEHOLDER COMMUNICATIONS

The following sections outline communications recommendations based on the different first responder possibilities. A FedRAMP ISSO will rarely, if ever, be a first responder because FedRAMP ISSOs are not users of the CSP system, and have no monitoring capabilities of any kind. A first responder must have the ability to notice or detect events on the system.

The path of incident communications will be different based on who happens to be the first responder.

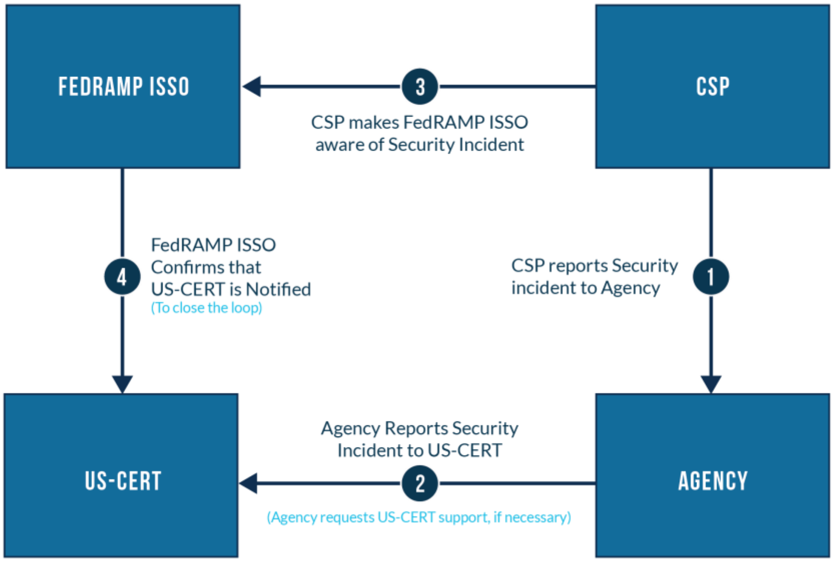
4.1. CSP IS THE FIRST RESPONDER, ONE AGENCY AFFECTED

If a CSP detects an incident that has the potential to cause an agency service availability disruption, a compromise of data confidentiality, or a compromise of federal data integrity, the CSP should proceed with notification to stakeholders in accordance with its incident response plan. CSP's should first notify the agency customer who has the potential to be affected by the incident. All agencies that receive CSP incident reports should ask the CSP if they would like assistance from US-CERT. If the CSP opts to request assistance from US-CERT, the agency should notify US-CERT and provide US-CERT with information on the CSP point of contact.

After agency notification is completed, CSPs should notify their FedRAMP ISSO. FedRAMP ISSOs will engage in a dialogue with CSPs to obtain all relevant information. The FedRAMP ISSO will make note of whether or not the CSP requested assistance from US-CERT. The CSP's FedRAMP ISSO will confirm that all affected agency POCs are notified of the incident. After communications with the CSP takes place, the FedRAMP ISSO will contact US-CERT to confirm that US-CERT has been made aware of the incident. FedRAMP ISSOs will engage in a dialogue with US-CERT to obtain all relevant information.

The FedRAMP ISSO will record information related to the incident in the FedRAMP database, and will monitor next steps. The process that should be used when a CSP is a first responder is illustrated in Figure 1.

Figure 1. CSP is the First Responder, Incident Affects One Agency


FEDRAMP ISSO
CSP
3
CSP makes FedRAMP ISSO aware of Security Incident
4
FedRAMP ISSO Confirms that US-CERT is Notified
(To close the loop)
CSP reports Security incident to Agency
1
US-CERT
Agency Reports Security Incident to US-CERT
2
(Agency requests US-CERT support, if necessary)
AGENCY

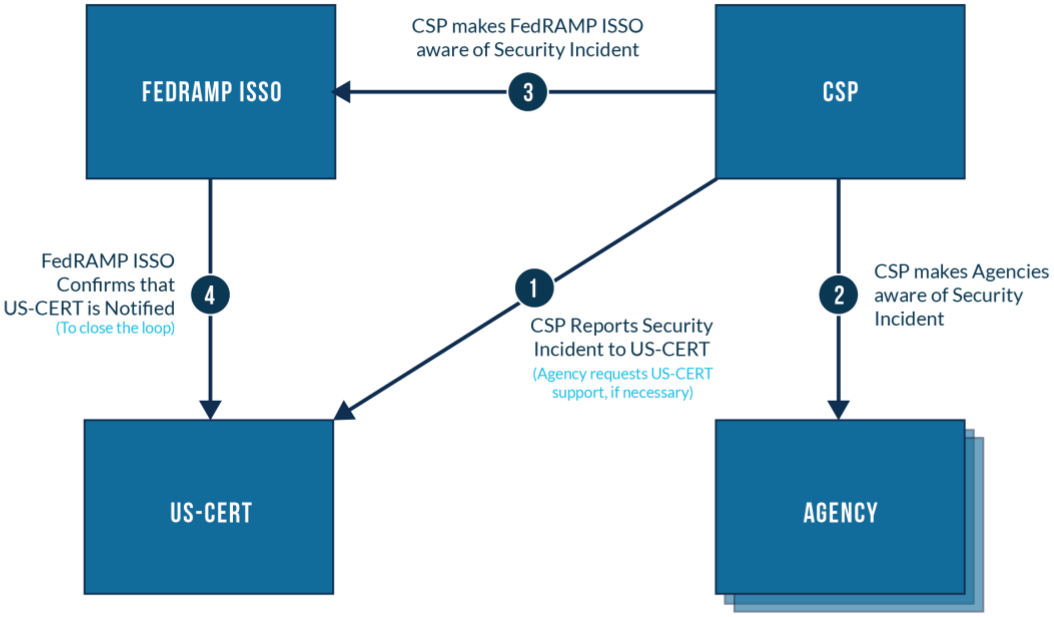
4.2. CSP IS THE FIRST RESPONDER, MULTIPLE AGENCIES AFFECTED

If a CSP detects an incident that has the potential to affect multiple agencies with either a service disruption, a compromise of data confidentiality, or a compromise of federal data integrity, the CSP should report the incident first to US-CERT. CSP's should advise US-CERT if they require assistance with the incident handling. CSP's should then notify the agency customers that have the potential to be affected by the incident.

After customer notification is completed, CSPs should notify their FedRAMP ISSO. FedRAMP ISSOs will engage in a dialogue with CSPs to obtain all relevant information. The FedRAMP ISSO will make note of whether or not the CSP requested (via agency customer) assistance from US-CERT. The FedRAMP ISSO will confirm that all affected agency POCs are notified of the incident.

The FedRAMP ISSO will record information related to the incident in the FedRAMP database, and will check monitor next steps. After communications with the CSP takes place, the FedRAMP ISSO will contact US-CERT to confirm that US-CERT has been made aware of the incident. FedRAMP ISSOs will engage in a dialogue with US-CERT to obtain all relevant information. The process that should be used when a CSP is a first responder is illustrated in Figure 2.

Figure 2. CSP is the First Responder, Incident Affects Multiple Agencies


FEDRAMP ISSO
CSP makes FedRAMP ISSO aware of Security Incident
3
CSP
FedRAMP ISSO Confirms that US-CERT is Notified
(To close the loop)
4
1
CSP Reports Security Incident to US-CERT
(Agency requests US-CERT support, if necessary)
2
CSP makes Agencies aware of Security Incident
US-CERT
AGENCY

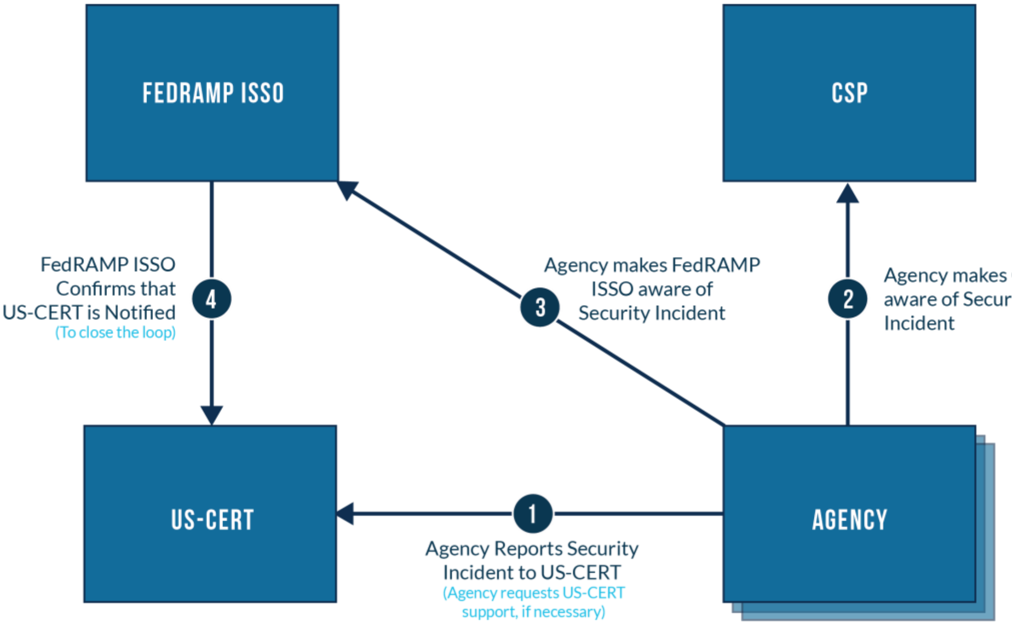
4.3. AGENCY IS THE FIRST RESPONDER

It is possible that an agency may become suspicious of activity they are seeing on their cloud platform before it is evident at the CSP monitoring center. An incident on an agency host sitting on a cloud system, completely local to the agency host, might be unrelated to anything happening below the hypervisor on the underlying cloud infrastructure. Agencies will want to confirm with the CSP whether that is the case or not. Agencies should take into consideration that incidents could occur on virtual machines due to reasons unrelated to the underlying cloud architecture.

When an agency is the first responder, it will notify its CSP of the suspicious activity or incident. The CSP should work with the agency to determine if the incident is local to the agency host (or hosts), or is part of a larger incident that affects the CSP's underlying cloud infrastructure – affecting multiple cloud tenants. After the agency notifies the CSP, it should notify the FedRAMP ISSO that is assigned to the CSP system and relay any pertinent information. After communications with the CSP takes place, the FedRAMP ISSO will contact US-CERT to confirm that US-CERT has been made aware of the incident. FedRAMP ISSOs will engage in a dialogue with US-CERT to obtain all relevant information. The agency should enlist the support of US-CERT according to the agency security policies and Incident Response Plan.

The FedRAMP ISSO will record information related to the incident in the FedRAMP database, and will monitor next steps. The process that should be used when the agency is the first responder is illustrated in Figure 3.

Figure 3. Agency is the First Responder


FEDRAMP ISSO
CSP
FedRAMP ISSO Confirms that US-CERT is Notified
(To close the loop)
4
Agency makes FedRAMP ISSO aware of Security Incident
3
2
Agency makes CSP aware of Security Incident
US-CERT
1
AGENCY
Agency Reports Security Incident to US-CERT
(Agency requests US-CERT support, if necessary)

4.4. US-CERT IS THE FIRST RESPONDER

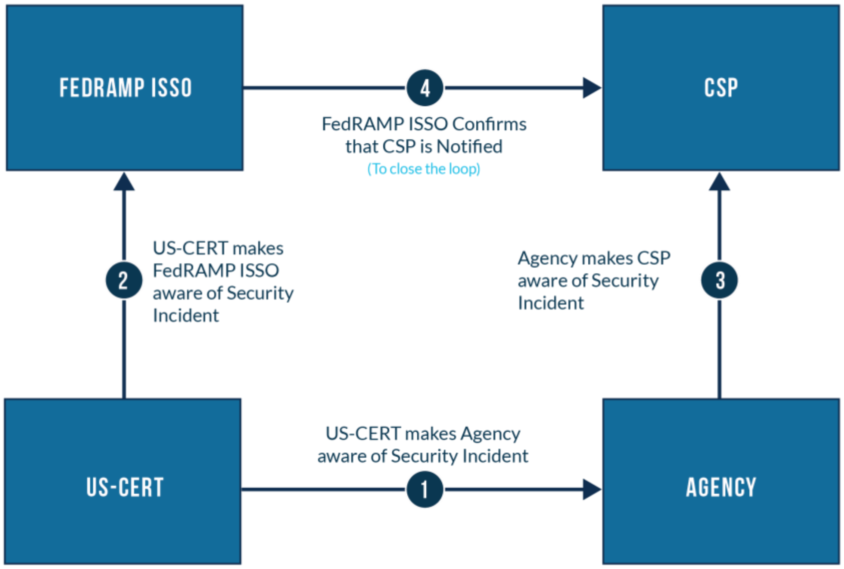
In certain circumstances, US-CERT may become aware of potential or real incidents before it has become evident to the CSP or the agency. US-CERT captures network flow data via sensors that enable them to correlate and identify malicious activity. Network anomalies discovered on traffic that traverses Trusted Internet Connections (TICs) is another mechanism that US-CERT uses to become aware of incidents. Additionally, US-CERT serves as a general incident response center for the U.S. government and the U.S. private sector, and as a result, often becomes aware of incidents sooner than other entities. US-CERT may want to bring malicious activity to the attention of agencies and their respective CSPs.

When US-CERT is the first responder, it will notify affected agencies of the suspicious activity or incident. US-CERT should work with the agency to determine if the incident is local to the agency, or is part of a larger incident that affects multiple agencies, and their underlying cloud infrastructures.

Working with the agency, US-CERT should ascertain whether the incident appears to affect an agency CSP. If a CSP appears to be affected, US-CERT then notifies the FedRAMP ISSO by sending an email to isso@fedramp.gov. The agency should notify its CSP and inform them of the malicious activity discovered by US-CERT. The FedRAMP ISSO will contact the CSP to confirm that they received proper notification from the agency and will monitor next steps.

The process that should be used when US-CERT is the first responder is illustrated in Figure 4. Various incident response scenarios are illustrated in Appendix A.

Figure 4. Agency is the First Responder


FEDRAMP ISSO
CSP
4
FedRAMP ISSO Confirms that CSP is Notified
(To close the loop)
2
US-CERT makes FedRAMP ISSO aware of Security Incident
Agency makes CSP aware of Security Incident
3
US-CERT
US-CERT makes Agency aware of Security Incident
1
AGENCY

5. THE SECURITY INCIDENT LIFE-CYCLE

The Security Incident Life-Cycle, illustrated in Figure 5, is composed of the following phases: Preparation, Detection and Analysis, Containment and Eradication, Recovery, and the Post-Incident Activities. Some of the life-cycle activities are performed in parallel with each other (e.g. analysis, communication and documentation).

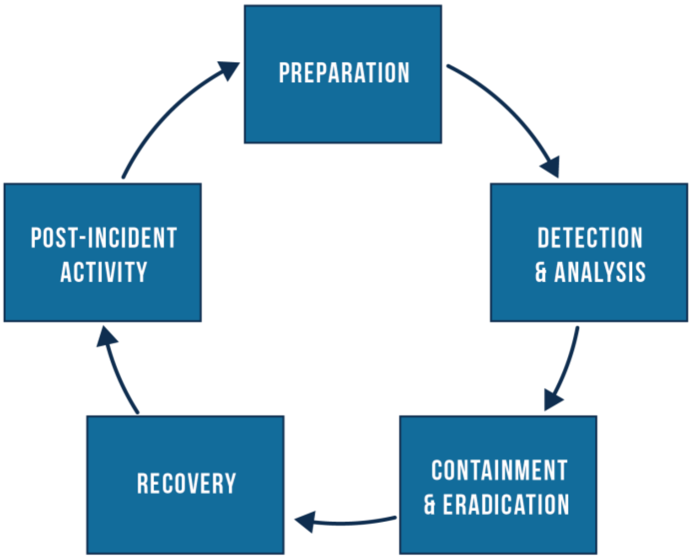
- **Preparation**: Maintaining and improving the first responder's incident response capabilities;

- **Detection and Analysis**: Detection, confirmation, and analysis of suspected incidents;
- **Containment & Eradication**: Minimizing loss, theft of information, or disruption of service, and elimination of the threat;
- **Recovery:** Restoring the computing services securely and in a timely manner;
- **Post-Incident Activity**: Assessment of the incident response to better handle future incidents through the utilization of logs review, “Lessons Learned” and after-action reports, or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.

In addition to the above listed activities, there are various cross-cutting elements which are always present throughout the Security Incident Life-Cycle:

- **Communication:** The FedRAMP ISSO must ensure that all stakeholders are notified as appropriate. Each stakeholder should have information that is consistent with other stakeholders.
- **Analysis:** All stakeholders should perform continuous examination of available data to support decision-making throughout the security incident life-cycle.
- **Documentation:** All stakeholders should record and time-stamp status information and any evidence obtained from detection through post-incident activity. If a forensic investigation is being performed chain of custody should be recorded.

Figure 5. Incident Life-Cycle



5.1. PREPARATION

When preparing for an incident, stakeholders should take into consideration the following questions:

1. What preparations have been made by the incident response team?
2. Has the Incident Response Plan been tested?
3. Are former Lessons Learned archived where all team members can access them?
4. Is the contact list in the Incident Response Plan up to date?
5. Does staff listed in the Incident Response Plan contact list have a copy of the plan?
6. What were past precursors of incidents?
7. What tools are available in house to perform incident handling?

5.2. DETECTION AND ANALYSIS

There are certain types of system and network activities that are often considered suspicious. Not all suspicious activity constitutes a security incident and should therefore be carefully researched and analyzed before any decisions are made.

When trying to determine if an incident has in fact taken place and what items require analysis, stakeholders should take into consideration the following questions:

1. What indicators caused someone to think that an incident might have occurred?
2. When did the problem start and is it still on-going?
3. Where did the suspicious activity take place? What servers and networks?

5.3. CONTAINMENT, ERADICATION, AND RECOVERY

Containing an incident means not letting it spread further to other systems and networks. Eradication refers to removing it completely. When handling an incident, initially, priority should always be given to containment. There may be reasons why eradicating an incident is not initially the right course of action. For example, if you eradicate the incident before performing forensics, you may not be able to identify the cause of the incident, or the perpetrator. If you want to perform memory forensics on a server, you cannot shut the server down, otherwise you clear out the memory on the server and you are left with nothing to analyze.

Decisions need to be made before an incident is eradicated on whether it is best to simply recover quickly, or perform advanced forensics. If the plan is to perform a forensic investigation for the purpose of identifying a perpetrator for prosecution, evidence needs to be preserved. If the incident is eradicated before evidence is preserved, then it is not possible to perform a forensic investigation.

When performing containment, eradication, and recovery, stakeholders should take into consideration the following questions:

1. What strategy should the organization take to contain the incident?

2. What could happen if the incident were not contained?
3. What additional tools might be needed to respond to this particular incident?
4. What sources of evidence, if any, should the organization acquire?
5. How should the evidence be acquired?
6. Where will the evidence be stored?
7. How long should evidence be retained?
8. Which team members should be involved in the containment, eradication, and/or recovery processes?

5.4. POST-INCIDENT ACTIVITY:

Post-incident activity refers to reviewing and reflecting on the recently closed incident for the purpose of preventing such incidents from occurring in the future.

When performing post-incident activities, stakeholders should take into consideration the following questions:

1. Who should attend the post-incident lessons learned meetings regarding this incident?
2. What could be done to prevent similar incidents from occurring in the future?
3. What could be done to improve the detection of similar incidents?
4. How many incident response team members participated in handling this incident?
5. Did we have the right people participating on the team?
6. How long did it take to close the incident once it was identified?
7. Besides the incident response team, what groups within the CSP were involved in handling and eradicating this incident?
8. What tools and resources did the team use in handling this incident?
9. What aspects of the handling might have been different if the incident had occurred at a different day and time (on-hours versus off-hours)?

What aspects of the handling might have been different if the incident had occurred at a different physical location (primary versus alternate site)?

APPENDIX A: INCIDENT RESPONSE SCENARIOS

The National Institute of Standards and Technology (NIST) *SP 800-61, Revision 2, Computer Security Incident Handling Guide*, provides various scenarios as an effective way to help organizations build their incident response skills and identify potential issues with their incident response processes. FedRAMP has created the following scenarios and questions with the recommended responses, so that each FedRAMP stakeholder can better understand their role during a security incident.

Each scenario below is followed by incident-specific questions and suggested responses. FedRAMP stakeholders are encouraged to adapt these scenarios and questions for use in their own incident response exercises. Note that the responses presented in these scenarios are for guidance only and in most cases will not represent the full communications dialogue in its entirety. The illustrative scenarios presented present only a subset of the communications required for each incident.

A.1. SCENARIO 1: DOMAIN NAME SYSTEM (DNS) SERVER DENIAL OF SERVICE (DOS)

On a Saturday afternoon, external users start having problems accessing an agency's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a staff member of the CSP's networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both of the CSP's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

The CSP should consider the following key questions:

1. Who should the CSP contact for more information on the external IP address in question?
2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?
3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

Recommended Responses

1. The CSP should contact their ISP for assistance. The customer agency should offer the CSP assistance from US-CERT and should contact US-CERT and provide to them the CSP POC so that US-CERT can reach out to the CSP.
2. The nine internal hosts should be taken off the network and scanned for malware. If none is found, but the problem still exists, the CSP should consider reimaging the hosts.
3. The CSP should review the log files on their DNS servers, routers, and firewalls to identify the two hosts.

A.2. SCENARIO 2: COMPROMISED DATABASE SERVER

On a Tuesday night, a CSP database administrator performs some off-hours maintenance on several production database servers. The administrator detects some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team's investigation determines that the attacker successfully gained root access to the server six weeks ago.

The CSP should consider the following key questions:

1. What sources might the team use to determine when the compromise had occurred?
2. How would the handling of this incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?
3. How would the handling of this incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including personally identifiable information) each night and transfer it to an external address?
4. How would the handling of this incident change if the team discovered a rootkit on the server?

Recommended Responses

1. The incident response team should review the system's log files.
2. All system passwords on the network should be changed immediately.
3. The external address should be blocked (blacklisted) and the database log files should be reviewed to determine if sensitive information has been compromised. The CSP should notify the affected customers immediately.
4. The CSP should ask their agency POC to request help from US-CERT, as this may have a wide-spread impact on federal customers.

A.3. SCENARIO 3: WORM AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. In the past, the CSP incurred widespread infections before antivirus signatures became available several hours after the worm started to spread.

The CSP should consider the following key questions:

1. How should the CSP incident response team identify all infected hosts?
2. How should the CSP attempt to prevent the worm from entering the system before antivirus signatures are released?
3. How should the CSP attempt to prevent the worm from potentially spreading before antivirus signatures were released?
4. Should the CSP attempt to patch all vulnerable machines? If so, how is this be performed?
5. How should the handling of this incident change if infected hosts (that had received the DDoS agent) had been configured to attack another entity's website the next morning?
6. How should the handling of this incident change if one or more of the infected hosts contained personally identifiable information?
7. How should the incident response team keep agency customers informed about the status of the incident?
8. What additional measures should the CSP team perform for hosts that are not currently connected to the network (e.g., staff on vacation that currently do not have their laptops connected to the network)?

Recommended Responses

1. The worm, after infecting a host, will try to scan neighboring IP addresses to find the next targets. Neighboring IP addresses can be a good place to detect if a host is infected with a worm. Generally, any legitimate program runs on a specific location on a network. Worms, on the other hand, need to find targets. If we monitor the number of IP addresses scanned by the host, and if it exceeds a certain threshold, then we can safely assume that a worm has been detected.
2. The CSP should make use of reputable Intrusion Prevention and Antivirus tools on all systems within the security boundary.
3. The CSP should aggressively quarantine any process that shows erratic behavior. After isolating the process, it should be monitored for a period of time corresponding to the erratic behavior shown by the process. If the process does not show any aberrant behavior during the time it's monitored, it can be released. If it shows the same behavior again and again, it is quarantined and labeled as a worm.
4. The CSP should have an active patch and update program in place, and should use the change management process documented in their Configuration Management Plan.
5. All agencies connected to the CSP should be made aware of the infestation, so that their incident response teams can activate to assess their systems and take remedial actions, if needed.
6. System log files should be reviewed to determine if any sensitive information has been compromised. The CSP should notify any affected customers immediately.
7. The CSP's incident response team should work with the FedRAMP ISSO to ensure all affected parties are notified.
8. Hosts not currently on the network, should be identified and scanned before being allowed to connect to the network.

APPENDIX B: FedRAMP ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.