

Incident Response Requirements and Process Clarification Comment Disposition and FAQ



11/27/2014



Table of Contents

1. Incident Response Requirements and Process Clarification Comment Disposition ...	3
2. Incident Response Requirements and Process Clarification FAQ	10

1. INCIDENT RESPONSE REQUIREMENTS AND PROCESS CLARIFICATION COMMENT DISPOSITION

Note: FedRAMP provided responses to substantive comments provided during the public comment period. Comments with suggested editorial changes are being considered and integrated along with other editorial changes submitted with the documents.

Comment	Response
<p>An agency could have a requirement that only designated persons from within the agency are authorized to report incidents to US-CERT, and having the CSP report directly to US-CERT would violate Agency policy.</p>	<p>In a cloud environment where a CSP may have an incident that affects multiple federal customers, it makes sense to file a single report to US-CERT rather than having all affected customers duplicate reporting. However, if the Agency does prevent the CSP from reporting directly to US-CERT, the CSP will need to document this and provide an incident response plan showing the process for incident reporting.</p>
<p>Comment: The FedRAMP cloud provider is employed directly or indirectly by a Government Agency. That Government Agency is responsible for incident response and the program office(s) and/or operational entity within said Agency responsible for cloud operations is ultimately responsible for any response necessary. There needs to be a requirement to the FedRAMP cloud provider that they must follow an incident response process mandated by their Federal customer. US-CERT is a means to provide awareness across all Government. However, US-CERT is not the acting incident response Agency for response action, incident impact analysis and mitigation all of which need to be started as soon as the cloud service provider detects what is believe to be an incident. Service level agreements templates should be made available to Federal Agencies so the cloud service providers can follow a standard process that is tailored to their Federal Agency customer.</p> <p>Reasoning: Programs within the Agency using the cloud provided service as an extension of their system need to have strategic knowledge of any impact involving their software. Any impact incurred on their software in the cloud</p>	<p>In a cloud environment where a CSP may have an incident that affects multiple federal customers, it makes sense to file a single report to US-CERT rather than having all affected customers duplicate reporting. However, if the Agency does prevent the CSP from reporting directly to US-CERT, the CSP will need to document this and provide an incident response plan showing the process for incident reporting.</p>

Comment	Response
<p>architecture directly impacts their service. This is no different than any restrictions required of a cloud provider on schedule maintenance. Although not scheduled, the impact of a cyber incident should require timely communications to the cloud customer that impacted by the incident in their cloud service. This way, discussion between the cloud provider and their customer can take place helping to lower the time of response and recovery. It is important that US-CERT receives the information but it is more important that direct and timely communications between the cloud service provider and the cloud customer takes place without having to go through a third party.</p>	
<p>I believe it is good you are augmenting your evaluation criteria.</p> <p>-Should the test case include a reference to the FedRAMP Incident Communications Procedure? Since that procedure document contains critical details of FedRAMP incident reporting requirements and scenarios, perhaps the tester can use the document as a reference point to compare it against the CSP’s documentation, and determine if the CSP’s documentation aligns.</p> <p>-For the last part of the test case, “Test incident response policies and procedures to ensure that the FedRAMP PMO and US-CERT are notified of all applicable incidents as part of the annual response testing”, are you instructing the tester to actually perform a simulated incident? I suspect you may be instructing the tester to examine evidence that annual response testing occurs and aligns with FedRAMP requirements. You can clarify the test case by elaborating on the instructions.</p>	<p>As part of the assessment, CSPs are required to review the FedRAMP Incident Communications Procedure and submit an incident communications plan for Review. While the Incident Communications Procedure is a useful document, the NIST control language and the test case language do not directly reference the Incident Communications Procedure.</p>
<p>Timelines are not specified in 800-61.</p> <p>NIST 800-61r2 indicates: Requirements, categories, and timeframes for reporting incidents to US-CERT are on the US-CERT website.</p>	<p>"As amended" refers to the most recent version of the document. This means we are refereeing to 800-61 r2.</p>

Comment	Response
<p>FedRAMP PMO is listed as a separate stakeholder from FedRAMP ISSOs in the FedRAMP Incident Communications Procedure.</p> <p>That Incident Comm Procedure indicates: CSPs should notify their FedRAMP ISSO.</p>	<p>The FedRAMP ISSOs are the part of the PMO that directly work with CSPs that have a P-ATO. The CSP is required to contact their ISSO.</p>
<p>Must assessor test or be part of the test? Or would 3PAO typically examine test results from the annual test?</p> <p>We think that the “examine” method is likely more appropriate than the “test“ method for this assessment procedure.</p> <p>Keep in mind that the FedRAMP Incident Communications Procedure s indicates and shows in diagram that CSP only contacts US-CERT if multiple agencies are affected (see section 4.2 of Incident Comm Procedure). Otherwise, the agency is the stakeholder to contact US-CERT.</p> <p>Is it really expected that FedRAMP and US-CERT “are” notified as part of testing? We think that a test (tabletop or otherwise) would indicate that FedRAMP and possibly US-CERT “would be” notified, but that a CSP does not perform actual notification if it’s only a test scenario, not an actual security incident.</p> <p>For example: Examine the annual incident response test results to verify that the FedRAMP ISSO and US-CERT would be notified of applicable incidents.</p>	<p>1.3PAOs are required to test incident response capabilities as part of the assessment. The 3PAO would produce the testing results used in the annual assessment.</p> <p>2. The test case language points to applicable incidents for ISSO and US-CERT notification.</p> <p>3. Yes, the 3PAO would only test the ability, not create an actual report to US-CERT during testing.</p>

Comment	Response
<p>There is no issue in examining policies, procedures and the IRP to identify the reference or required reporting times to US-CERT. Testing for reporting of real or potential breaches results in examining records of lessons learned and reviewing the history of any incidents. The 3PAO can ask to examine records and time stamping of the identified incident and subsequent reporting to FedRAMP and US-CERT, but unless an incident is publicly known or clearly identified by an IR ticket, the 3PAO may not be able to identify incident and the time of the notification.</p> <p>- Test incident response policies and procedures to ensure that the FedRAMP PMO and US-CERT are notified of all applicable incidents as part of the annual response testing.</p> <p>Comment: The guidance needs clarification. IR-3 in Continuous monitoring suggests that the test results are documented in the FedRAMP template. The artifact related to notifying US-CERT may be difficult – and if misinterpreted by CSP personnel could result in notification overloads to US-CERT.</p>	<p>Testing the incident response policy and procedures may be a table-top exercise led by the 3PAO to see how the CSP manages incident response reporting. Results of all testing are documented in the Security Assessment Report FedRAMP template. Testing should not require actually submitting a report to US-CERT.</p>
<p>Recommend citing specific requirements or providing specific sections within NIST SP800-61.</p>	<p>FedRAMP will consider this change.</p>
<p>Recommend being more specific. Reporting requirements should be as specific as possible. The requirements seem vague and are not entirely clear.</p>	<p>The test language needs to account for different policies and procedures based on the CSP, therefore the language needs to be broad enough to allow the 3PAO to assess the control for different systems and CSPs.</p>
<p>This will give you a sampling, but it doesn't seem necessarily scientific. Perhaps recommending all people complete a questionnaire and reviewing the findings to gather more objective results/statistics.</p>	<p>Even if the 3PAO issues a questionnaire, it may only be distributed to a sampling of people with incident reporting responsibilities depending on the size of the CSP.</p>

Comment	Response
<p>The same wording is used repeatedly. From structure standpoint, since some of the wording is being reused it is recommended to state it once introducing the thought and then expanding for each sub-component. i.e. “Examine incident response... or other relevant document regarding how they apply to 1. Organizational incident response capability 2. Organization-defined authorities 3. Notification process to FedRAMP PMO & US-CERT 4. Reporting security incident information to authorities, etc.</p> <p>Recommend being as specific as possible (i.e. sampling of malicious logic/infection or misuse incident).</p>	<p>FedRAMP is using a format for test cases similar to the test cases issued by NIST. NIST's documentation format is considered the standard for test cases.</p>
<p>Recommend providing guidelines how IR policies should be tested. Should this be done in the form of an exercise? If this is a requirement then it is recommended to be specific</p>	<p>It's up to the 3PAO to determine exactly how to test these requirements. The test methodology is documented in the SAP and approved by FedRAMP or the agency AO.</p>
<p>What is being done to account for existing SLAs with the IR framework? - There is nothing in the document speaking to IR SLAs. There is mention reporting timelines, but nothing on notification, confirmation and resolution of incidents. If the problem is stakeholders not being kept in the loop regarding security incidents by their CSPs, enforcing SLAs is a good way to ensure that communication channels remain open, and that vital IR data is being disseminated in a timely, and efficient, manner.</p>	<p>Standard CSP SLAs many not cover Federal reporting requirements. FedRAMP published control specific contract guidance than addresses IR-6 incident reporting requirements.</p>
<p>(a) Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and</p> <p>US CERT provides guidance for this via the following link: https://www.us-cert.gov/government-users/reporting-requirements</p>	<p>This control language specifically addresses reporting internally within the CSP. That time frame would be defined by the CSP, but would also need to be in line with US-CERT reporting externally.</p>

Comment	Response
<p>CSPs are responsible for reporting incidents to customers that result in an actual or reasonably suspected unauthorized disclosure of Customer Data. This may not include all security incidents, if the incident does not impact Customer Data.</p> <ul style="list-style-type: none"> ○ As such, some of the US-CERT incident categories may not impact Customer Data and thus the CSP does not have a responsibility to report these to the customer. 	<p>FedRAMP agrees, CSPs would report incidents that include the disclosure of Federal customer data, but there are still other incidents, such as an outage, that may impact the customer and should be reported to the agency and FedRAMP. While not all incidents will have an impact on the customer, some incidents may indicate a change in the CSP's security posture. The agency should define which incidents they are interested in being notified about. Also, unclear how CSP is determining within acceptable reporting timeframes if customer data is impacted.</p>
<p>CSPs have contractual obligations and customer privacy requirements that make direct reporting to entities other than those designated by the customer infeasible.</p>	<p>If the agency has contractual requirements for the CSP to report incidents to US-CERT, it would be feasible. ATO and P-ATO require reporting on incidents. CSPs should work with customers to update contracts or choose appropriate ATOs to align with their contracts.</p>
<p>The applicability of US-CERT incident reporting timeframes for reporting of incidents should be clarified by US-CERT. The purpose of the US-CERT reporting timeframes is to allow US-CERT and DHS to assist the agency with the investigation. The US-CERT reporting timeframes apply to Federal agencies and do not directly apply to CSPs who are identifying and responding to security incidents. Reporting timeframes for CSPs should be specified in CSP customer contracts.</p>	<p>US-CERT reporting timeframes are a Federal requirement for agencies. CSPs wanting to work with the Federal government will need to support the agency's ability to meet this reporting timeframes if Federal data or Federal systems are impacted by an incident affecting a CSP.</p>
<p>The Cloud Service Provider is responsible for reporting incidents to customers that result in an actual or reasonably suspected unauthorized disclosure of Customer Data. As a service provider, the CSP is responsible for managing its infrastructure and security practices. When an incident is impactful to a customer, the CSP is responsible for reporting it. Other non-customer impacting incidents are not reported to customers.</p>	<p>FedRAMP agrees that CSPs would report incidents that include the disclosure of Federal customer data, but there are still other incidents, such as an outage, that may impact the customer and should be reported to the agency and FedRAMP. While not all incidents will have an impact on the customer, some incidents may indicate a change in the CSP's security posture. The agency should define which incidents they are interested in being notified about.</p>

Comment	Response
<p>Cloud Service Providers have a direct relationship with their customers (Resellers of CSP services may contractually make the CSIP a 3rd party to the customer). As such communication of security incidents is limited to the CSP and the customer. Limiting communications from the CSP to the customer is necessary for contractual reasons to ensure that customer data is protected and not shared with third party entities. The customer is responsible for identifying a customer point of contact to be notified in the event of an incident, which could include Agency Security Points of Contact (i.e. Agency Incidents Response Teams, Authorizing Officials).</p> <p>Once the customer has been notified of a security incident, the customer can then report the security incident to third parties that they have a responsibility to report to (such as US-CERT or the FedRAMP PMO). These are contacts that are designated/mandated by the customer for security incident reporting. The customer is directly responsible for reporting to these third party entities.</p>	<p>In a cloud environment where a CSP may have an incident that affects multiple federal customers, it makes sense to file a single report to US-CERT rather than having all affected customers duplicate reporting. CSPs will also need to be able to notify FedRAMP of incidents that impact Federal customers and the CSP's ability to respond to incidents is a requirement of maintaining FedRAMP compliant ATO.</p>
<p>Through review of the current the US-CERT categories (https://www.us-cert.gov/government-users/reporting-requirements), as it relates to cloud service offerings and discussions with US-CERT, incidents involving an actual or reasonably suspected unauthorized disclosure of Customer Data will be communicated promptly to the customer, in accordance with contractual obligations between the CSP and the customer, regardless of the US-CERT Category. Government agencies (customer) are then responsible for reporting any incidents that involve an actual or reasonably suspected unauthorized disclosure of Customer Data identified by the CSP to US-CERT in accordance with designated US-CERT reporting timelines.</p>	<p>In a cloud environment where a CSP may have an incident that affects multiple federal customers, it makes sense to file a single report to US-CERT instead of having all affected customers duplicate reporting. CSPs will also need to be able to notify FedRAMP of incidents that impact Federal customers and the CSP's ability to respond to incidents is a requirement of maintaining FedRAMP compliant ATO.</p>

2. INCIDENT RESPONSE REQUIREMENTS AND PROCESS CLARIFICATION FAQ

Question	Response
<p>Are the below listed requirements only for reporting incidents involving CSPs?</p>	<p>This test language is mostly targeted to a CSP in testing their system during a FedRAMP assessment. While this language is mostly targeted at CSPs, it may have some impact on the agency depending on customer responsibilities and CSP service model.</p>
<p>Is the stated reporting requirement handled by the DHS SOC (i.e. all components report to DHS SOC & DHS SOC then reports incident), or is this a 'new' requirement whereby the components each handle the reporting per incident?</p>	<p>This requirement is to ensure that the AO and FedRAMP are notified of incidents. Individual agencies may have slight variations on how they respond to incidents. If the DHS requirement is to report to the DHS SOC, then that requirements stands for DHS.</p>
<p>How is the appropriate "organization" identified? Is this FedRAMP, the D/A using service, etc.?</p>	<p>The control language and test cases are mostly meant for the assessment of CSPs, so the organization here would be the CSP.</p>