

Vulnerability Scanning Requirements and Process Clarification Comment Disposition and FAQ



11/27/2014



Table of Contents

1. Vulnerability Scanning Requirements and Process Clarification Comment Disposition.....	3
2. Vulnerability Scanning Requirements and Process Clarification FAQ.....	14

1. VULNERABILITY SCANNING 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>I agree that you need consistent results between an independent assessment and Continuous Monitoring. However, there is some benefit to using different scanners. One scanner might pick up vulnerabilities that a different scanner did not find. If both scanners have CVE listings, it should be possible to map one scanner vulnerability ID to that of another scanner. If a 3PAO decides to use a crappy scanner that does not find as many vulnerabilities, it would actually be a good thing for the CSP to use a better scanner. I would caution against sending the message, “If your 3PAO used a crappy scanner, be sure to use the same crappy scanner for Continuous Monitoring.” It is more trouble to do the mappings from one scanner to another, but it actually increases the prospect of finding vulnerabilities by using multiple scanners.</p>	<p>FedRAMP concurs with your general comments concerning scanning and the use of scan tools.</p>
<p>On Page 2, under RA-5 VULNERABILITY SCANNING CONTROL, steps for the organization have been identified. Steps D and E talk about ‘Remediation of legitimate vulnerabilities’. After remediation is done, how does the organization ensure that the remediation has, in fact, fixed the vulnerabilities and it is effective?</p> <p>Suggest the need to include one more step after –</p> <ul style="list-style-type: none"> · Rescan for vulnerabilities - to ensure that the vulnerabilities identified and remediated were indeed taken care of and the report to be shared and kept on file. 	<p>FedRAMP concurs with your comment and will consider adding the rescanning language to the test case.</p>

Comment	Response
<p>I'm surprised that CA-5 for Plan of Action and Milestones isn't listed as a related control. Our POA&M is mostly based on our vuln scan results from RA-5. Our POA&M is how we track our success (or lack thereof) for RA-5d in terms of remediating the vulnerabilities within the FedRAMP required timeframes</p>	<p>Listed related controls are quoted directly from NIST 800-53 Rev. 4. FedRAMP Cannot change NIST's control language.</p>
<p>It doesn't seem that CSPs should really be assessed for evidence of identifying new vulnerabilities that may affect their systems (such as Heartbleed). The RA-5 control text doesn't state a requirement to identify such new vulnerabilities. The control requirement is in relation to *when* the scans must occur, which would be soon after new vulnerabilities are identified.</p> <p>I interpret this as scan monthly, but you may have to scan between those monthly iterations if a new vulnerability (like Heartbleed) is identified.</p> <p>For this RA-5 control, I think the goal is *awareness* of new vulnerabilities that other orgs (likely external) have identified (see SI-5 control), and then scanning in a more timely manner due to that awareness and availability of a corresponding "plug-in" for the scanner that will allow detection of that new vulnerability.</p>	<p>FedRAMP will consider changing the wording. FedRAMP wants insight into what the CSP is going to do (i.e. what the process is) if they find, for example, a new zero-day exploit. In particular, that they are going to notify the FedRAMP PMO and US-CERT. The other parties that may be notified are up to the CSP and their agency customer.</p>
<p>Keep in mind that RA-5(1) is for ability to update scan tool to check for new vulnerabilities, and RA-5(2) is for frequency to update scan tool.</p> <p>RA-5 is about *when* to scan. However, the RA-5a wording is vague and prone to varying interpretation. New vulnerabilities are frequently identified, but we don't scan every time a new vulnerability is identified. We scan monthly except when a major new vulnerability that's being exploited (like Heartbleed) is identified.</p>	<p>Mostly concur. FedRAMP agrees the wording could be improved; however the wording came straight from NIST. "Planned" scans should be run as described in the SSP, but ad-hoc and other scans should also be run. Updates should be installed each time the scanner is run and new vulnerabilities should be scanned at the earliest opportunity.</p>
<p>The personnel who conduct the scans and assessments may not be the same personnel for analyzing those scan and assessment results.</p>	<p>I concur. They'll both have to be interviewed, in that case.</p>

Comment	Response
<p>I think the POA&M shows evidence of remediation. An individual scan report or assessment doesn't show evidence or remediation. It's a set of consecutive scan reports or assessments that can show that previously indicated vulnerabilities are no longer present. Closed POA&M items seem like the most obvious evidence of remediating vulnerabilities.</p>	<p>FedRAMP concurs, POA&Ms come under the category of "other relevant documents" and should be examined. However, it is uncontroversial to suggest that the assessor needs to determine whether or not remediation is being performed within the required timeframes.</p>
<p>1) Maybe clarify where configuration management and patch management evidence might be found if not within the vulnerability scanning/management evidence typically associated with RA-5. For example, assessment of CM-9 and/or SI-2 might be helpful in terms of showing linkage to RA-5 if RA-5 doesn't show linkage to them.</p> <p>2) "Test" method, as in assessor actually being granted access to use our scanning tools? Or is it sufficient to have assessor compare results from our use of our scanning tools with results from their use of their scanning tools to verify consistency? It seems the "examine" method might be sufficient and more efficient.</p> <p>3) RA-5a: Group the frequency related cases together.</p> <p>4) RA-5a: Group the process related cases together (this is vulnerability scanning process, as opposed to the vulnerability management process that is mentioned repeatedly later in the cases).</p> <p>5) RA-5a: There are a couple cases related to a process for identifying and reporting new vulnerabilities. It seems that process is beyond the scope of RA-5 assessment and seems more related to SI-5. RA-5 is about scanning when vulnerabilities have been newly identified, but RA-5 is not about how those new vulnerabilities actually got identified and got their associated plug-ins, CVEs, etc. CSPs use tools that work with the new plug-ins to check our own systems for the presence of the newly identified vulnerabilities, but CSPs aren't held responsible for finding ways to discover those</p>	<p>FedRAMP had a great deal of discussion about what should (or should not) be grouped. We had several criteria, such as who is performing the action (that is, we didn't want to group together things that were the responsibility of the assessor with things that were the responsibility of the CSP), and so on. We'll look at this more closely and see if we can make any improvements.</p>

Comment	Response
<p>new vulnerabilities such that we can then scan for them.</p> <p>6) RA-5a: It might help to clarify the conditions for “when” we must truly conduct intermediate scans with reported results between the monthly scan reports that we know we need to comply.</p> <p>7) RA-5b: It looks like there are 11 cases associated with the RA-5b control text about tools and techniques that “facilitate interoperability” and “automation” by “using standards”. How many of those cases must really be employed if the scan tools being used by the CSP are well known and documented as being SCAP-validated? SCAP is all about interoperability, automation, and standards. If the tool is SCAP-validated, then what more is needed beyond valid scan results that are consistent with the 3PAO’s results as proof of such standards in use for the interoperability and automation benefits that are desired?</p> <p>8) RA-5c: (analysis of scan reports) Consider specifying “output from analysis”, rather than “measures to analyze” as evidence of measures being applied. Also consider which personnel should be interviewed because those conducting the scans may not be the ones responsible for the analysis and monthly reporting. For example, our security compliance group (SPPO) may hire a vuln scanning team to run the scan tools, but our compliance group is ultimately responsible for analyzing the results produced by the scanning team and produced by the 3PAO scans and SARs. Our compliance group does the monthly reporting to FedRAMP based on the analyses of those scan reports.</p> <p>9) RA-5d: (remediates) Third and fourth cases associated with RA-5d don’t even mention the POA&M as a relevant artifact to be examined. It seems that the POA&M provides very appropriate evidence of the measures to be applied to remediate vulnerabilities and evidence as to whether those measures are being applied. More importantly, the fourth case doesn’t specify checking for evidence of</p>	

Comment	Response
<p>timely remediation. The control text covers specifics about timeframes for remediating based on risk designation, so there should be a case specified for the assessor to examine evidence to determine whether the CSP is or is not remediating vulnerabilities within their expected timeframes from date of discovery.</p> <p>10) RA-5e: (shares info) Consider specifying which measures are being assessed. We have the same concern earlier in the document as well (measures for analysis, measures for remediation, etc.). There are so many cases stated but various different measures are relevant for different cases. Specifying which measures are being assessed for a given case would be helpful clarification and could avoid some confusion or misinterpretation.</p>	
<p>Recommend listing periodic security posture checks/scan, not necessarily linked to the three listed processes. Referencing only the three listed may inadvertently restrict the attention or focus of what is required.</p>	<p>FedRAMP disagrees. This is a non-exhaustive list. The words "such as" imply "including but not limited to."</p>
<p>Recommend stating as many specific requirements that need to be met when an assessor and/or CSP performs a vulnerability assessment. It is recommended to make requirements that can be met using various scanning tools (i.e. minimum FISMA scan policy, full credentialed scan, etc.)</p>	<p>FedRAMP tries to be as specific as possible, but test cases need to apply to a wide variety of systems and environments. Therefore, we may not include an exhaustive list.</p>
<p>Recommend expanding list of network connected devices to include all end-nodes, including network infrastructure devices (i.e. routers, switches, load-balancers, firewalls etc.).</p> <p>Recommend such things as secure code review by development team when dealing with custom coded applications.</p>	<p>FedRAMP disagrees. The words "such as" imply "including but not limited to." We do agree about the code analysis, but that is covered below and in other controls.</p>

Comment	Response
<p>Cite specific requirements needing to be met for all of the below listed checks/cases as they are associated with other authoritative sources (i.e. NIST SP800-40 and/or SP800115) Recommend citing specific examples or a process to follow to further outline the requirement needing to be met. Recommend requiring full credential/authenticated scans when performing system OS scans. Recommending providing a specific process of how this is to be done.</p>	<p>FedRAMP concurs on running credentialed scans whenever possible, and will try to insert some wording to that end. There may be better places to do that, however.</p>
<p>As written it appears the 3PAO is working with another independent assessor. My interpretation is that the FedRAMP office wants to have consistent – similar testing between the organization’s in house security team (or outsourced security team) and the 3PAO. It didn’t convey this to us without multiple readings.</p> <p>Using similar testing and similar configurations amongst the 3PAOs and the continuous monitoring program provides standardization and comparative capabilities. It also has the potential weakness of reducing the ability to see risk from new perspectives. Testing from time to time with different tools provides validation that the tools and the system do not have unknown undiscovered vulnerabilities. As written, when implemented, new exploits not captured by old tools could become an issue if the 3PAO and the CSP do not use or update to new tools on a periodic basis (3-5 years).</p>	<p>FedRAMP will look at the wording and see if we can improve it.</p>
<p>Examine a sample of vulnerability scan reports for the information system and hosted applications for evidence that the measures are being applied to conduct vulnerability scans in accordance with the process." - Not knowing what kind of sample, or in what timeframes these samples will be taken, could pose a problem for those systems that are application residing on a GSS such as TOP. Since application scans are only done within a six month period, rather than monthly, this sample could be small, and perhaps not as informative as it might be for systems that are scanned on</p>	<p>These test cases apply to systems that must be scanned (and have other activities) on a variety of schedules. This test, among other things, simply asks the assessor to ensure that the schedule is appropriate and that scanning is being performed to that schedule.</p>

Comment	Response
a monthly basis.	
3rd paragraph: Recommend adding "asset management" and "account management" to the minimum list of processes with linkage to the "vulnerability process". - Accurate asset mgmt is a prerequisite for accurate configuration mgmt. Account management is essential wrt vulnerabilities associated with user access attack vectors, insider threats, and more.	Concur that an accurate inventory is critical, but that is covered in other controls.
CDM requirement is every 72 hours.	FedRAMP does not require CSPs to scan every 72 hours. FedRAMP may consider the integration of CDM requirements at some time in the future.
Analyzes vulnerability scan reports and results from security control assessments; And prioritizes high risk vulnerabilities first or provides a vulnerability impact	Concur, though that is covered in another test case.
There is no reference to the required control enhancement, namely (1), (2) & (5).	This control language was pulled directly from NIST SP 800-53 Rev. 4. FedRAMP cannot change NIST's control language.
<p>Monthly Operating System (OS), monthly web applications, and monthly database vulnerability scans (and as needed)] .</p> <p>Monthly scanning is not consistent with the CDM 72 hour currency. Scans should be more frequently even if there is only monthly reporting of results.</p>	The FedRAMP PMO is working with DHS to harmonize FedRAMP and DHS requirements for CDM.

Comment	Response
<p>Test that the entity performing vulnerability scans in continuous monitoring has configured the scanner</p> <p>This is easy enough to do, but who produces the benchmark that asserts it is configured correctly? Is it configured correctly or is it configured to mimic the independent assessors tool?</p>	<p>The FedRAMP PMO is working with DHS to harmonize FedRAMP and DHS requirements for CDM.</p>
<p>Is producing reports in an appropriate manner (authenticated, updated definitions, full range and depth), consistent with that of the independent assessor’s reports.</p> <p>This is not an easy task. For example, they would need to know what tool the independent assessor was using and determine what vulnerabilities both tools are actually checking against. Then they would need a way to have their output fill in “voids” in a manner that would make it consistent with the assessors output.</p> <p>For example, if the CSP tool checked for CVE-X, but the independent assessors tool did not, -results sample of configuration assessment difficult to obtain the desired information easily. Does it mean to make their report consistent? What about the reverse, the assessors tool checks for CVE-Y but the CSP tool does not...seems the CSP report would have to have an entry for that CVE, and all the associated devices with platforms affected by the CVE, and label it as “unchecked”.</p> <p>Most sites do not know for certain what vulnerabilities the tool checks for – you have to get that explicitly from the vendor and have it continually updated.</p>	<p>While it may not always be an easy task, CSPs must be able to produce consistent scan results in order to maintain their FedRAMP compliant status.</p>
<p>Interview a sample of organizational personnel with vulnerability scanning responsibilities for the information system for further evidence that the measures are being applied.</p> <p>This would only be necessary if the application was not evident from the assessment reports.</p>	<p>FedRAMP requires this interview to ensure that the CSP is following its own documented processes.</p>

Comment	Response
<p>Examine documentation and a sample of configuration assessment results describing the current configuration settings for a sample of the mechanisms for evidence that these mechanisms are configured to facilitate interoperability among the tools. Examine documentation describing the current configuration settings for a sample of the mechanisms that automate parts of the process for enumerating platforms, software flaws, and improper configurations for evidence that these mechanisms are configured as required.</p> <p>Documentation or assessment results? I can write a document about how it should be configured or I can assess the configuration...the second one produces the desired evidence.</p> <p>Where is the continuous monitoring with automation of Configuration Settings?</p>	<p>FedRAMP agrees. This test case requires the review of both documentation and assessment results for this test to be comprehensive.</p>
<p>Examine documentation and a sample of configuration assessment results describing the current configuration settings for a sample of the mechanisms that automate parts of the process for formatting checklists and test procedures for evidence that these mechanisms are configured as required.</p> <p>Documentation or assessment results? I can write a document about how it should be configured or I can assess the configuration...the second one produces the desired evidence.</p>	<p>FedRAMP agrees. This test case requires the review of both documentation and assessment results for this test to be comprehensive.</p>
<p>Test a sample of the mechanisms and their configuration settings that automate parts of the process for enumerating platforms, software flaws, and improper configurations; conducting testing for evidence that these mechanisms are operating as intended.</p> <p>This does not say to test the mechanisms to see if they are configured correctly, but to provide evidence that the appropriate automation is occurring. No-where are the configurations checked in the operational environment.</p>	<p>FedRAMP agrees. This test case only tests the automation. There is another test case that tests the operational characteristics.</p>

Comment	Response
<p>Furthermore, there is a consensus between industry and the government that reporting vulnerabilities with a low risk designation provides little value with respect to the evaluation of the CSP’s security posture or compliance with FedRAMP requirements.</p>	<p>While we certainly concur that more resources and effort should be (and is) placed on high and moderate impact vulnerabilities, FedRAMP requires that CSPs report all known vulnerabilities.</p>
<p>NIST 800-115 discourages reliance on a scanner provided risk rating as the authoritative determination of the severity of a vulnerability. - "...the risk levels assigned by a scanner may not reflect the actual risk to the organization—for example, a scanner might label an FTP server as a moderate risk because it transmits passwords in clear text, but if the organization only uses the FTP server as an anonymous public server that does not use passwords, then the actual risk might be considerably lower. Assessors should determine the appropriate risk level for each vulnerability and not simply accept the risk levels assigned by vulnerability scanners."</p>	<p>FedRAMP currently has a process for the adjustment of risk items that requires approval by the AO.</p>
<p>NIST 800-53, RA-5 and the associated assessment cases expect a CSP to implement risk assessment policies and procedures that include the measures to be employed to analyze vulnerability scan reports and results from security control assessments. - “Examine risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents for the measures to be employed to analyze vulnerability scan reports and results from security control assessments.”</p>	<p>The requirements of the risk assessment are based on the risk tolerance of the Federal data owner.</p>

Comment	Response
<p>NIST 800-53, RA-5 and the associated assessment cases expect a CSP to implement procedures for assigning risk designations to all legitimate vulnerabilities as a result of an organizational assessment of risk. - “Examine risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, risk assessment methodology, security plan, or other relevant documents for the risk designations to be assigned to all legitimate vulnerabilities as a result of an organizational assessment of risk. Examine risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, risk assessment methodology, security plan, or other relevant documents for the organization-defined response times assigned to the risk designations in order to remediate legitimate vulnerabilities assigned to these risk designations as a result of an organizational assessment of risk. [high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate-risk vulnerabilities mitigated within ninety days from date of discovery]”</p>	<p>While a CSP may perform the risk assessment, the AO decides the risk tolerance for the Federal Agency and the JAB sets the risk tolerance for FedRAMP.</p>
<p>The DHS National Vulnerability Database recommends the use of the CVSS framework to assign risk ratings to vulnerabilities identified as a result of vulnerability scans. The framework recognizes that a scanner only provides the base CVSS score which should be adjusted for operational context. - http://nvd.nist.gov/cvss.cfm?calculator&version=2</p>	<p>DHS is one of the members of the JAB and has input into FedRAMP requirements. Use of the DHS National Vulnerability Database Framework is not required by FedRAMP.</p>

2. VULNERABILITY SCANNING REQUIREMENTS AND PROCESS CLARIFICATION FAQ

Question	Response
<p>There are various specific aspects of the process addressed in subsequent test cases, so I question the usefulness/need for a test case related to the generic process as a whole.</p> <p>The NIST control doesn't mention the vuln scan process except in relation to sharing info from it.</p>	<p>Thanks for your input. We will consider your comment in the review of the test case.</p>
<p>Is this really a test? It seems more like an examining of results to check for consistency.</p>	<p>FedRAMP will consider changing the wording, but we do think the test is effective. 3PAOs should run their own scan and compare the results to those the CSP are getting during their monthly/quarterly scans.</p>
<p>What test cases really apply to the "newly identified" aspect of RA-5 that won't be covered by RA-5(1) and RA-5(2)?</p> <p>If the wording can reflect a test case that isn't already covered, then it seems appropriate to keep paragraphs along those lines. However, this paragraph and the ones prior to and after it seem too vague to serve as useful test cases beyond those for the RA-5 enhancements.</p>	<p>The CSP defined the process by which they scan for new vulnerabilities, FedRAMP is seeking confirmation that they are following their own processes. FedRAMP will consider clarifying the language.</p>
<p>Which measures?</p>	<p>This is standard NIST language and refers to the measures discussed in the control itself.</p>
<p>Is this test case important? What would it show beyond what the next 3 test cases show? The use of the standards is supposed to facilitate interoperability, so if the standards are configured, then interoperability is supposedly facilitated.</p> <p>However, interoperability isn't enough. The new test case is to check for consistency between the tool and results from continuous monitoring in relation to the tool and results from the independent assessor.</p>	<p>Concur. FedRAMP will consider removing this test case.</p>
<p>Is this really something the assessor would "test"? Wouldn't it suffice to example a sample of scan results to see if those results enumerate platforms, software flaws, and improper configurations?</p>	<p>One of the challenges in writing these test cases was distinguishing between testing that controls were implemented and operating as intended versus, for example, testing that the seed of the encryption algorithm was truly random. 3PAOs and CSPs can reasonably be expected to do the former, but not the latter.</p>

Question	Response
<p>Examining the scan reports and assessment results that are inputs for analysis doesn't really help as evidence of analysis. Wouldn't this be examining a POA&M, for example, which is composed as the output from analyzing scan reports and assessment results?</p>	<p>This may be a wording issue. The CSP has defined a process by which the "scan operator" performs analysis (for example, to eliminate false positives). All we want to see here is that they're performing the analysis properly and that the results are as intended.</p>
<p>What is meant by, "Examine a sample of vulnerability scan reports for the information system and hosted applications for evidence that the measures are being applied to conduct vulnerability scans in accordance with the required frequency."? - Not knowing what kind of sample, or in what timeframes these samples will be taken, could pose a problem for those systems that are application residing on a GSS such as TOP. Since application scans are only done within a six month period, rather than monthly, this sample could be small, and perhaps not as informative as it might be for systems that are scanned on a monthly basis.</p>	<p>These test cases apply to systems that must be scanned (and have other activities) on a variety of schedules. This test, among other things, simply asks the assessor to ensure that the schedule is appropriate and that scanning is being performed to that schedule.</p>
<p>"Test that the entity performing vulnerability scans in continuous monitoring has configured the scanner and is producing reports in an appropriate manner (authenticated, updated definitions, full range and depth), consistent with that of the independent assessor's reports."</p> <p>Who is going to be testing the scanner configs? How often will the scanners be checked? Who is responsible for maintaining the scanning tools used for these vulnerability scans? How does this impact third-party systems with limited support? What steps are necessary in order to determine that the scanners are in an acceptable state to perform vulnerability scans?</p>	<p>The 3PAO is responsible for a) understanding the CSP's plans, policies, and procedures, and b) ensuring that CSP personnel are following those plans, policies, and procedures. Therefore, in this instance, the 3PAO would be responsible for determining whether scanning is being done properly, and in accordance with organizational guidance.</p>
<p>Is SCAP requirement and/or RDMS needed? It provides uniformity and will allow for future automation of feeds to the AO in the form of dashboards that would be capable of displaying CVE, CCE, CPE, CWE for CSPs.</p>	<p>This control language was pulled directly from NIST SP 800-53 Rev. 4. FedRAMP cannot change NIST's control language.</p>