FedRAMP Comments on Draft NIST SP 800-53 Revision 5

Submitted by: Matt Goodrich - FedRAMP Director, GSA
Via: sec-cert@nist.gov
Date: September 12, 2017

FedRAMP welcomes the opportunity to comment on the public draft of NIST Special Publication 800-53 Revision 5 (r5). One of FedRAMP's key missions is to streamline the process for Federal agencies, Cloud Service Providers (CSPs), and Third Party Assessment Organizations (3PAOs) following the NIST Risk Management Framework (SP 800-37) and implementing the security controls needed to protect Federal information (NIST SP 800-53). In that spirit, our comments for the 800-53 revision 5 (hereinafter referred to as "r5") outline lessons learned from FedRAMP's transition from SP 800-53 revision 3 (r3) to SP 800-53 revision 4 (r4) transition, and suggestions from our industry partners on more efficient and effective ways to convey these types of overarching change to the industry.

FedRAMP's key focus in providing these comments is not to debate the validity or necessity of specific security and privacy controls, but to identify ways in which the burden of implementing r5 can be reduced for Federal agencies, vendors (both cloud and non-cloud), and the auditor community which must assess and validate that these controls are in place.

PROBLEM STATEMENTS

What is the true scope and impact of change of r4 to r5? For systems that are already authorized at r4, are they less secure than systems authorized at r5? If so, what are the critical control implementations, documentation, and evidence (assessments) that need to be implemented rapidly in order to ensure systems housing Federal information are adequately protected?

As a positive first step, NIST has provided redlined changes to the textual elements of controls from r4 to r5 and tables identifying which controls have been changed, added, or deleted. However, NIST has not provided any analysis of the defined the scope and impact of these changes for each control in the following ways:

- System documentation
- System operating environment, and
- System architecture.

This is more complicated because the security controls used to be organized by management, operational, and technical requirements. These three new categories (bulleted above) are not well defined in order to truly separate and understand the importance between each category from a security perspective, at each baseline and data categorization level.

FINDINGS AND QUESTIONS

FedRAMP believes that in order for r5 to be implemented in the most efficient and effective manner, NIST must identify the true scope of the r4 to r5 transition, provide rationale for the changes in a more granular way, and clearly articulate the full impact of this update to all stakeholders.

FedRAMP feels that without an associated guide for assessing the security controls it is difficult to evaluate the potential value of NIST's proposed changes. If the Tables and Appendices within the document are the means to assess transition impact, We recommend that NIST elaborate within the document, or in an associated 800-53a, the most efficient way to analyze and assess impact and risk, and ultimately ascertain the value using the Tables and Appendices. At the individual control level (or even holistically at the baseline level) the r5 changes do not include any rationale for change, basis for evaluation of the impact of the change (e.g. assessment test cases), or expectation setting for levels of effort (LoE) when transitioning from r4 to r5.

There are three key areas that require NIST clarification in order to provide for an effective and efficient transition to r5: (1) more details for new and updated controls, (2) rationale for deleted controls, and (3) how to streamline documentation of the controls implementation statements within the System Security Plan (SSP).

More Details For New and Updated Controls

R5 provides new and updated controls from r4. NIST has provided a documented rationale for why changes were made holistically to the security controls, however the rationale does not address the changes at the granular, control level. NIST went through exorbitant efforts to update this catalog of security controls – one control at a time. However, without providing context for each control change, stakeholders are left to question and wonder why specific changes to controls were made and guess what the real impact of these changes are during their transition.

FedRAMP believes NIST must address the following areas for new and updated controls:

- **Priority.** What is the priority of implementation of new controls and updated controls? Are all new and updated controls considered to have the same positive impacts on security and should be treated equally? Based on FedRAMP's review, this is not the case.
    - FedRAMP believes NIST must provide a prioritization of the new and updated security controls.
- **New Security.** In the overview of r5, NIST discusses how r5 introduces "New Security" concepts with the updated and added security controls. What are these "New Security" concepts and why are these important to this r5 set of baselines?
    - FedRAMP believes that NIST must clearly articulate what the "new security" concepts are and what controls specifically reflect this.
- **New/Updated Controls.** Are these new and updated security control descriptions based on new security objectives? Without understanding what the objectives are, how are agencies and vendors going to be sure they meet the intent of security controls if not meeting a security control explicitly as stated? Without the objectives, it is difficult to understand if alternate implementations or mitigating security controls are sufficient.
    - FedRAMP believes that NIST must provide security objectives for each control to clearly articulate the intent of each control so alternate implementations and mitigating controls can be properly analyzed.
- **Test Cases.** Where is the 800-53 r5 test case guidance (update to 800-53a)? Without test cases, there is no clear way to validate the implementation of the security controls and determine the level of effort for all stakeholders (agencies or vendors to implement and document, and auditors to assess the implementations).
    - FedRAMP **strongly** believes that NIST must release updates to 800-53a for public comment at the same time as r5.
        - When r4 was released, there was a delay between the release of r4 and the updated test cases within 800-53a. FedRAMP had to undertake creating test cases with our audit community in lieu of specific guidance from NIST. This took months and countless hours of work across government and industry.[1] NIST then released an updated 800-53a months after FedRAMP completed our test case workbook. The lack of guidance and uniformity between the release of these two

[1] It is safe to estimate the total cost of this was ~$250,000 just to develop the test cases without NIST having released an update to 800-53a for r4. To FedRAMP directly, we estimate the cost was anywhere between $100,000 to $150,000 dollars (650 to 800 hours at an average rate of $175/hour). Indirectly, to our 3PAO community whom we engaged for assistance, we estimate the cost at ~$100,000. The 3PAOs estimated they spent anywhere from $25,000-$30,000 worth of effort and we engaged 5 of our 3PAOs for this effort.

documents creates undue burden on Federal agencies and vendors – both in terms of significant cost and time.

- **Keywords.** What is the true intent of "keywords"? Is it merely guidance, is it to help support future automation capabilities, is it mandatory language to be included within a response in the SSP, or a combination of the above?
    - To make keywords more user-efficient, FedRAMP believes NIST must clearly state the intention of the keywords in Appendix H and how they should be applied by agencies and vendors.
        - For example, if these keywords are the precursor to NIST-defined automation schema - will these "Keywords" need to be included in the relevant security control implementation descriptions in all System Security Plans so that the document is machine-readable? If that is the is the case, NIST should be explicit about this.
    - Additionally, it appears as though the implementation of "keywords" has not been fully flushed out. Appendix H tells agencies that they need to do the full analysis to see if privacy controls are related to security controls.[2][3] What is the power and/or purpose of the keywords if agencies are still going to be doing the work individually to determine their effectiveness?
- **Technical Implications.** Citing new and updated controls, how has security changed, technically, that drives the control changes? If there is a control baseline change, why?
    - Specifically, why has the baseline for Low criticality level increased in number of controls, while Moderate and High criticality levels have decreased in number of controls?
        - FedRAMP believes strongly there are too many security controls at the low impact baseline and any addition at the low level will drive more vendors away from Federal business.
        - Additionally, it is unclear why the numbers are lower for moderate and high impact baselines – an articulation of why the number is lower will aid agencies and vendors in understanding what the holistic changes to the baseline mean for security.

[2] pg 13, "To maintain awareness and support collaboration between privacy and security programs, organizations may use the keywords in Appendix H to locate privacy references in security controls that are not designated as joint controls."

[3] pg 382, "Keywords can be used when searching for controls or control enhancements that may contain similar content or have a similar purpose."

Rationale for Deleted Controls

As part of the review and release of r5, NIST chose to delete some controls that were previously required for agencies and vendors to implement. It is unclear why those controls were deleted.

- **Deletions.** Why are controls dropped from the baselines? What is the rationale for deletion and what is the rationale for some of these being incorporated into other controls?
    - FedRAMP believes stakeholders need rationale regarding why a security control was previously required and now is not required in the baseline (e.g. Is this control no longer providing adequate security? Do new security controls cover that attack vector, etc?)

How to Streamline Documentation Within the SSP

NIST states that the language changes within r5 are made for clarity and understanding--that the changes will "have no effect on the actual security and privacy controls."[4] However, many of the additions/deletions to controls, or their explanations, exhibit substantive word choices, which seem to fundamentally change agencies' and vendors' ability to crosswalk current operations and new requirements for operations.

- **Documentation Updates:** If there are controls with no substantive changes to the intent or implementation (i.e., only textual changes), what is the expectation from NIST in reflecting the new language of the control within the SSP?
    - FedRAMP strongly believes that if NIST statements about these controls are true, then there is no reason for any stakeholders to need to update documentation simply to reflect the r5 changes if it does not impact security.
        - NIST must provide a list of this type of control so stakeholders can avoid unnecessary updates and effort that are not related to increasing the security of systems.
        - FedRAMP also strongly believes that if there are no substantive changes to the intent or implementation of a control, then at a minimum, the old assessment test cases and evidence should also be considered sufficient.
- **Versioning Controls**: FedRAMP believes that NIST should start "versioning" controls instead of doing holistic and wholesale changes to the 800-53 catalog of controls to eliminate the need for unnecessary updates in documentation.

[4] NIST SP 800-53 Revision 5: Status Update Projected Publication Date For Initial Public Draft, March 28, 2017.

- FedRAMP believes that this would *drastically* reduce the LoE related to the updates from revisions of 800-53 and would also allow for more frequent updates.

DOCUMENTATION LOE AND COST ANALYSIS

Due to the limited review time and the noted lack of information related to scope of changes detailed above, FedRAMP looked at a sample set of controls to determine the potential impact. The results of this analysis provides information that underscores the importance of a control-by-control scope and impact analysis, which would allow organizations to plan appropriately. The sample controls chosen were in both r4 and r5 baselines. The textual changes from r4 to r5 were analyzed to determine the impact of the changes.

- **60% of the controls only had minor word changes**. These changes were mostly to the Supplemental Guidance, where revised wording adds clarity without changing the intent of the control. These controls we believe would not require any changes to the System Security Plan (SSP).
- **40% of the controls *added* new or *modified* existing requirements and/or parameters.** At a minimum, these will require updates to the SSP and supporting plans (e.g. documents like the Incident Response Plan). Some of the new requirements/parameters may also require low-impact changes to management or operational procedures, if they are not already being met.

Based on our sampling, we assume approximately 40% of the r5 moderate baseline controls will require organizations to perform some sort of documentation update.

Based on our work transitioning from r3 to r4 and with discussions FedRAMP has had with our 3PAO and CSP community, we estimate the impact of the transition from r4 to r5 to at minimum involve the following LoE and cost for moderate impact systems:

- Vendor LoE and Cost
  - Technical Writer - 2 hours per control @ $125/hr = $28,750
  - SME Reviewer - 1 hour per control @ $175/hr = $20,125
- Agency LoE and Cost
  - Technical Reviewer - 2 hours per control @ $150/hr = $34,500
- FedRAMP LoE and Cost
  - Technical Reviewers (multiple reviewers) - 4 hours per control @ $150/hr = $69,000

Total estimated cost per system (CSP and Government review):

- Agency ATOs ($83,375) to JAB ($117,875)

Total cost to FedRAMP PMO and JAB:

- $69,000 @ 30 JAB authorized systems = $2,070,000

These cost totals ***only reflect*** documentation updates based on the sampling of FedRAMP's reviews. This does ***NOT*** include any additional costs associated with system upgrades that might be required due to r4 to r5 updates or any additional assessment test cases and reviews, including by third parties. Due to this, we believe the estimates above are very low estimates, and if anything might be less than half of what the total cost to implement these changes might in aggregate once vendors upgrade their systems, implement new controls, and have auditors/3PAOs independently verify these updates.

CONCLUSION

From the FedRAMP PMO perspective, we do not believe that we can more fully estimate or understand the true impact of r4 to r5 without more information provided by NIST as detailed above. Even with our estimation of 40% of controls having some sort of change at the moderate level, that will have an exorbitant impact on vendors and Federal agencies, and in particular FedRAMP - even only at the documentation level.

As FedRAMP saw with the the r3 to r4 transition, the biggest impact to all stakeholders was the consequential drag on operations created by (i) excess documentation; (ii) the burden of implementing new or changed security controls, (iii) the unclear plans for how to implement r5 changes, and (iv) NIST not clearly prioritizing r5 changes. This was compounded by the fact that it wasn't clearly articulated in a tangible way what the real security changes were that necessitated the update.

All four of these items created the biggest toil and cost for government and vendors for the transition from r3 to r4, and are still in place in the current r5 documentation.

In order to fully address our comments above and reduce the toil and burden that was experienced in prior updates to 800-53, FedRAMP suggests that NIST complete the following before r5 becomes finalized:

Provide a Gap Analysis for Low, Moderate, and High Baselines

FedRAMP asks, once r5 is the "rule" for security, what will be the projected scope and schedule of changes for all users? FedRAMP suggests that NIST provide a r4 to r5 gap analysis for the Low, Moderate, and High baselines that addresses the concerns noted in this paper. This gap analysis can be used by the stakeholders to determine what must be implemented to maintain their system at the currently prescribed risk posture or potentially lessen their risk level.

NIST Must Release 800-53a (Assessment Test Cases) with 800-53 r5

In order to truly understand impact, NIST must release the new 800-53r5 test cases along with the final r5. Otherwise, NIST is releasing the requirements without the details on how to ensure the requirements are being met. This will create a drag on time and resources for all parties involved to actually implement r5 in a timely manner and to plan for total cost and impact for agencies and vendors.

APPENDIX A: SUPPORTING DISCUSSION

QUESTIONS FROM STAKEHOLDERS

The following are a synopses of questions that FedRAMP has been fielding from the FedRAMP stakeholders related to r5. Each section represents a stakeholder group at a very high level of questioning. However, there are pervasive themes within each section.

The transition severely impacts time and resources but it is not clear if the transition affects the level of security and risk.

If I am a CSP...

1. I want to know how to interpret these 800-53r5 changes as these apply to my CSO and my organization.
2. Are these documentation changes or do I have to change operations?
3. Do I need to update my system architecture?
4. The security I have on my system is sufficient at the 800-53r4 level as evidenced by my P-ATO or my ATO. What do I need to change to make my system 800-53r5 compliant?
5. If my system was tested against 800-53r5 standards today, what security controls are going to be deficient?
6. What is the rationale behind making these changes to make my system compliant to r5 when everything is sufficient at r4? (Adage applies, "if it's not broken, don't fix it".)

If I am a 3PAO...

1. I need to know how I am going to change my testing criteria for my CSPs and my Agencies.
2. Where is 800-53Ar5 testing criteria? I cannot gauge with total accuracy how NIST/FedRAMP expects these new baselines to be implemented without testing criteria.
3. This will affect my Quality Management System. That will be a significant increase which will affect the cost to my customers.
4. This will affect my internal pricing structure. Are the changes substantive so that I must add testing resources?
5. Will extra time be required for testing an 800-53r4 compliant system (for the Low, Moderate, and High baselines) against 800-53r5 baseline?
6. If I have systems that are low risk at a r4 moderate baseline, how does this change with the r5 baseline?
7. There are more controls for the Low baseline but there are less controls for the Moderate and High baselines. Does this mean that the moderate and high systems now have an overabundance of security?

8. Will FedRAMP add more controls to these r5 baselines? We would rather make changes all at once than piece by piece since this piecemeal effect cost a huge amount of resources (money and personnel) for r3 to r4 transition.

If I am an Agency…

1. How do I estimate security assessment costs for FY 18?
2. Will this r4 to r5 transition increase or decrease my system annual assessment cost by 20%? By 30%?
3. Conversely, will this change truly decrease my cost since there are less security controls (Moderate and High baselines)?
4. Will less security controls required in a specific baseline detract from the level of security required for my system?
5. How does this change to r5 affect my system stable risk posture assuming that my Authorizing Official is comfortable with the current system risk posture?
6. What controls will I have to change to accommodate the r5 compliance?
7. Is there an easy way to use the documentation that you have provided within the r5 draft, for instance, to allow me to estimate the cost of transition?