RECOMMENDATION ONE: Normalize JAB and Agency ATO Certification Processes

Problem Statement	FedRAMP Response
CSPs view the JAB certification process as the gold standard. As a result, not all FedRAMP ATOs are seen as equal — which fundamentally undermines the value proposition of the program. This perception has driven an increased volume of CSP certification packages through the JAB process, creating a bottleneck of certification packages that must be managed by a program office that is understaffed and underfunded to handle the volume — the program is no longer scalable. Agencies often refuse to accept other Agency ATOs. Some agencies also bypass FedRAMP by leveraging "in progress" certifications from companies that have simply submitted their first round of documentation. What is the relative value of a JAB ATO, an agency ATO, and a CSP supplied package? Are they all the same? The value of the three types of ATO must be made clear if we are to preserve the benefit of reuse.	FedRAMP was designed to standardize the process of assessments and the ability to analyze risks of systems. It was not meant to standardize the risk of systems. The JAB, made up of the CIOs of the Department of Defense, Homeland Security and the General Services Administration, understandably has a very low tolerance for risk when it comes to information security. To that end, the JAB asks that any vendor who wants to store, process or transmit this information meet the strictest standards for security. CSPs who meet this threshold are designated as meeting security requirements and are recommended for use throughout the government. Each agency has its own risk tolerance based on their mission, (think FEMA vs Secret Service, and both are within DHS). Individual system implementations have to take into account their specific risks when determining the applicability of a particular ATO. This reflects the broad scope of the Federal government's services and missions and gives appropriate flexibility as allowed under FISMA and the NIST framework. Part of our efforts to reduce the backlog was to update the security control revision 3 to revision 4 updates. While clearing out the backlog, the PMO with the JAB teams performed a redesign of the authorization process (FedRAMP Accelerated) that address many of the concerns detailed below, increases reliance on 3PAOs for CSP success, and the PMO launched a dashboard with greater visibility into CSP status and expected authorization dates for systems in process. This is the first year that the FedRAMP JAB has received funding. We have been working diligently to reduce the backlog of work for CSPs currently in the program, and launched a FedRAMP Accelerated pilot to test whether CSPs can move through the process within a 6 month timeframe.
Recommended Actions	**FedRAMP Response**
Establish a capacity baseline for the FedRAMP PMO and JAB process based on current resourcing levels to determine the number of CSP certification packages that can be processed in a year. Refine how CSP packages are	The JAB and PMO are developing a capacity model that includes criteria on prioritization. A public survey was released to stakeholders and interested parties, including industry, on September 2nd and information

selected and prioritized for the JAB to review. Publish these metrics and selection criteria.	captured from that survey will be used to assess ways to further maximize the capacity and throughput of the FedRAMP approval process. Additionally, FedRAMP has published a dashboard to transparently show where CSP certification packages are in the process (marketplace.fedramp.gov).
Develop a clearly defined process for upgrading Agency ATOs to a JAB ATO when governmentwide demand is shown.	This is indeed a part of the prioritization criteria mentioned above. As a note, it is and always has been voluntary for a CSP to migrate their offering from an Agency ATO to a JAB ATO and we expect to work with CSP's to determine when such an "upgrade" is prudent.
Establish Service Level Agreements to be met by FedRAMP PMO JAB.	As we iterate to a more efficient, accelerated process, we plan to incorporate SLA's and manage the work throughput accordingly. For now, as we prove FedRAMP Accelerated, work plans are generated and agreed to between CSPs and the JAB when initiating any authorization activities.
Quantify and define what constitutes a material deficiency in a CSP submission package. This should be supported by a published checklist of non-negotiable controls, clear expectations for control implementation, and alternative implementations.	These controls and checklists are currently available on FedRAMP.gov and offered to prospective CSP's at initial contact with the PMO. It is important to note that some CSP deficiencies are due to an overall number of deficiencies – not just one "go/no-go" deficiency (the sum of all is greater than just one).
Engage the Cloud Computing Caucus to help reinforce through governmentwide policy channels and, if necessary, agency budget channels, the fact that FedRAMP is not an aspirational program, but mandatory.	FedRAMP engages directly with Agencies and a range of groups, including ACT/IAC, ITAPS, PSC, academia, and the CIO Council, to better understand their needs of the process/program. We expect that the engagement with this caucus will continue to increase over time as the program expands. OMB, as the policy owner, is responsible for enforcing FedRAMP compliance across agencies.
Use an online tool to provide greater transparency into the status of CSP packages. The tool should provide, at a minimum, the status of the package in the FedRAMP review process (JAB and Agency), and the projected review timeline. Use online tool to publish ATO deployment data, including reuse, cost, and customer satisfaction. Consider a public-private partnership with existing resources, such as the FedRAMP OnRamp.	FedRAMP addressed this request by launching an online marketplace with this information on FedRAMP.gov in August 2016 at marketplace.fedramp.gov
Ensure agencies and CSPs have access to training and information that facilitates the submission of complete packages for review.	FedRAMP provides checklists for package submission, free training sessions via FedRAMP.gov as well as direct access to FedRAMP PMO personnel to answer questions of any type. These resources are available to everyone.

RECOMMENDATION TWO: Increase Transparency

Problem Statement	FedRAMP Response
Nobody can say for sure exactly how much a JAB ATO costs a CSP to achieve, but we do know it takes too much time and a lot of money. In addition, how and why CSPs get into the pipeline, and how the FedRAMP PMO prioritizes reviews, is a mystery and creates the perception that the government is choosing the winners and losers. The FedRAMP PMO and the Hill need to take an active role to demystify the cost, and sell the value of the program to agencies and industry. In light of the horror stories about the cost of attaining an ATO for CSPs, the continued lack of transparency on how a company interacts with the PMO and the continued lack of understanding of what it takes to win will lead industry to stop signing up to the process. Further, if the Hill does not enforce the FedRAMP requirement, why would industry and government agencies sign up to the process? Industry needs to be more transparent about the real costs involved in gaining certification. But for industry to do that, the FedRAMP PMO must first develop an incentive program that facilitates information sharing on best practices. Likewise, the FedRAMP program lacks a champion. While the recent hiring of its first "Evangelist" is a step in the right direction, the long-term goal must be to demonstrate publicly where FedRAMP is delivering value. This can only be achieved by detailing where CSPs are providing cloud services and the benefits those services are bringing to agencies. This falls to both the CSPs and the FedRAMP PMO to collect and publish this data.	The FedRAMP PMO is working with several CSPs to better understand their costs and create an ROI model by which CSPs can identify the cost of obtaining an ATO. Additionally, the new Readiness Assessment Report is designed for CSPs to better understand their capabilities and if they meet the needed requirements for FedRAMP prior to entering the full assessment process. This relies more heavily on the 3PAOs – something that CSPs and 3PAOs have expressly asked for and recommended for greater efficiency. The JAB is redefining the prioritization criteria in order to match the growth of the program. This criteria will be released within the next 60 days. FedRAMP is working closely with OMB to increase OMB's visibility, oversight and championship of the program and will work closely with the Technology Transformation Service Commissioner to detail the quantifiable value that FedRAMP provides to its constituents. The FedRAMP PMO does not have the authority to enforce FedRAMP or to create incentive models – that is an OMB responsibility as the policy owner. The dashboard, marketplace.fedramp.gov, provides transparent information into agency participation in the program which can help OMB enforce participation. Additionally, CSPs who do not follow FedRAMP will have a harder time moving from agency to agency for procurements. Industry bears the responsibility of meeting Federal requirements in order to gain maximum reciprocity and use.
Recommended Actions	**FedRAMP Response**
Establish parameters to better understand how CSPs are spending their FedRAMP investment dollars.	FedRAMP worked with providers to get a better understanding of the costs associated with submitting a Cloud Service for review. This cost assessment was posted to the Focus on FedRAMP blog on September 8. Additionally, a comparison of the historical process against FedRAMP Accelerated will be generated and published once the current Accelerated pilot is complete.
The FedRAMP PMO should work with CSPs, the FedRAMP Fast Forward Industry Advocacy Group, and	FedRAMP meets with OMB on a weekly basis to address program issues and OMB is responsible for oversight and

the Office of Management and Budget to collect and share more information about FedRAMP ATO CSP current deployments and success stories, as well as to increase engagement on FedRAMP oversight. Leverage oversight and new authorities granted under the Federal Information Technology Acquisition Reform Act (FITARA) to develop incentives for greater agency information sharing on in-progress and finalized ATO packages.	enforcement of the FedRAMP program. In addition to the creation of the FedRAMP evangelist positon and recent increase in public information sharing via industry days, the press, GSA blog posts, dashboard (marketplace.fedramp.gov) and interactions with industry groups, The Focus on FedRAMP blog on FedRAMP.gov is a new avenue for FedRAMP to share additional FedRAMP success stories, new and improved features and more information to our stakeholders overall.
Coordinate with 3PAOs to develop and publish a webinar series of high-value training covering real-world examples of how CSPs accelerate through the ATO process.	FedRAMP already provides a free training program available via FedRAMP.gov and will work with 3PAO's, CSP's and other constituents to refine this capability over time.
Leverage the CIO Council Knowledge Portal to enable agency information sharing on best practices and effective governance.	FedRAMP has launched government-only agency roundtables and will work with agencies to determine the best place to share information (like on max.gov) based on agency requests and preference.
Identify a senior executive within the General Services Administration (GSA) to lead communication effort and strategic initiatives.	This executive exists in the form of the Technology Transformation Service Commissioner and has also appointed a senior executive to serve in this role for FedRAMP, the FedRAMP Agency Evangelist Ashley Mahan.
Increase customer outreach to identify issues that require guidance from the PMO.	While this is a responsibility of the TTS Commissioner and FedRAMP PMO Director, this is the primary responsibility of the FedRAMP Agency Evangelist. On a weekly basis she talks to an average of 10 agencies and 5 vendors. We are also using the FedRAMP blog to keep vendors informed. In addition, there is a marked increase in industry days, listening sessions and industry consortium interactions from and with the entire FedRAMP/GSA executive team.
Deploy a post-process customer questionnaire to collect information from CSPs on customer satisfaction and process issues. To obtain real, meaningful feedback from CSPs, we need to set up a non-profit public-private entity to solicit and anonymize CSP responses.	In coordination with A2LA, we are setting up a post process questionnaire for our 3PAOs. We have also deployed a post process questionnaire for all FedRAMP ATOs. We do not believe a non-government entity is needed to collect this information.

RECOMMENDATION THREE: Harmonize Industry Standards

Problem Statement	FedRAMP Response
CSPs have invested heavily in certifications against a large number of international security and privacy standards, including ISO/IEC 27001, the Health Insurance Portability and Accountability Act (HIPAA), and the Criminal Justice Information Services (CJIS) standards, to name just a few. A series of industry groups have already mapped these standards to the FedRAMP requirements, but the FedRAMP PMO does not recognize CSPs for their compliance with these standards.	Mapping of standards is the first step in this process for harmonization. The evidence associated with the controls is more important than just the mapping of security controls to each other. For instance the CAG 20 actually relates to over 170 NIST security controls. Additionally, while ISO has a policy requirement around username and passwords – there isn't any specific requirement for details of the passwords – a provider could enforce a policy that all passwords be 1234512345, which would pass ISO requirements but would not pass FISMA requirements. FedRAMP believes that the large effort to harmonize standards is something that should be led by industry -- or potentially the Federal CISO or NIST -- however, auditors and CSPs have the experience of complying with the various standards. They are the ones who have the greatest knowledge of how standards overlap and would be the group best suited for proposing how various standards could be better harmonized. FedRAMP's rigorous standards and details around secure implementations are being used in other regulated industries and has allowed many FedRAMP authorized providers to become major players in other industries as well.
Recommended Actions	**FedRAMP Response**
Incorporate into the existing FedRAMP ATO process a means by which CSPs can meet certain FedRAMP requirements through their compliance with existing international security and privacy standards to help speed up the process and reduce redundant costs to the government and industry.	We believe this is something that should be industry led. FedRAMP is currently working with DOD to present a position paper for industry to detail the problem and request help from industry to solve.
Expand the pool of available 3PAOs by recognizing existing industry security accreditations.	We are currently examining the 3PAO requirements and will be updating them with the help of NIST and A2LA.
Rely on standards published by the National Institute of Standards and Technology (NIST) to ensure security and privacy requirements are maintained.	FedRAMP is 100% based on NIST standards.
Engage the Federal Inspector General community, working through the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to harmonize the	FedRAMP regularly engages with the CIGIE on issues related to FedRAMP.

auditing process, particularly for the audit plans put forth by Third-Party Assessment Organizations (3PAOs).	
Require CSPs and 3PAOs to document their actions during each phase of testing and certification to improve visibility and dialogue with the IG community.	There is a documented project plan and deliverables for all phases of a FedRAMP authorization.
Fix the FedRAMP process/system and champion FedRAMP as a standard for use across regulated industries and adjacent industries — state and local government, education, health care, and financial services — and to other governments on the international stage.	FedRAMP is championed by GSA as the premier security standard for cloud service providers. We regularly engage with NASCIO and governments from other nations about FedRAMP.

RECOMMENDATION FOUR: Reduce Cost of Continuous Monitoring

Problem Statement	FedRAMP Response
Per OMB policy, ongoing assessment and authorization is now the law of the land in Federal security. As a result, the FedRAMP program developed a continuous monitoring strategy for CSPs that have achieved an ATO. However, as its name implies, continuous monitoring is continuous and, therefore, costly to operate and maintain. Change management has become a real problem for FedRAMP, as CSPs make changes to their hardware and software, or discover new vulnerabilities that must be remediated. Significant changes require CSPs to submit security impact analyses to their Authorizing Official (AO), as well as testing and a reassessment by the 3PAO.	FedRAMP is actively investigating ways to find efficiencies for both government and industry in completing continuous monitoring. Similar to the effort of FedRAMP Accelerated, the FedRAMP PMO will undergo a redesign of continuous monitoring. This will be closely coordinated with the DHS CDM office and involve heavy interaction with vendors and 3PAOs.
Recommended Actions	**FedRAMP Response**
Empower authorized CSPs and 3PAOs to self-accredit changes and use continuous monitoring to validate security determinations.	This would require policy changes to NIST and DHS guidance.
Leverage a risk summary report prepared by the 3PAO to document the accrediting of CSP security processes.	This is already a part of the authorization process (the Security Assessment Report). Additionally, the Readiness Assessment Report also gives a good summary of CSP capabilities.
Establish a multi-stakeholder group to address issues of broad impact, such as information security continuous monitoring, reauthorizations of new functionality, Trusted Internet Connection (TIC), and governmentwide procurement vehicles. Deliver recommendations to OMB.	FedRAMP regularly engages with various stakeholder groups to address key issues, including the FedRAMP agency roundtables. In last meeting the TIC office participated, and agencies discussed ConMon.
Move FedRAMP ATO continuous monitoring from the FedRAMP PMO to the Department of Homeland Security.	Continuous Monitoring is the responsibility of CSPs. The analysis of continuous monitoring and acceptance of continued risk and changes to an authorization remain with the authorizing officials of a system. Transferring responsibility for Continuous Monitoring to DHS would require changes to NIST requirements and FISMA.

RECOMMENDATION FIVE: Empower Infrastructure Upgrades

Problem Statement	FedRAMP Response
CSPs that provide Infrastructure-as-a-Service (IaaS) struggle with finding the right balance between the demands of maintaining upgrades to their environments while remaining in compliance with FedRAMP. Furthermore, agencies don't understand what rules apply to IaaS versus Platform-as-a-Service (PaaS) versus Software-as-a-Service (Saas).	All systems that store, transmit, or process Federal information must have a security authorization. FedRAMP has defined change management processes and procedures – see recommendation 4 for planned enhancements.
Recommended Actions	**FedRAMP Response**
Work with the National Institute of Standards and Technology (NIST) and others to develop FedRAMP options for Infrastructure-as-a-Service (IaaS) providers, and create a lighter approach for Software-as-a-Service (SaaS) providers that sit on FedRAMP-compliant infrastructure.	It is unclear what "other options" means for IaaS providers. FedRAMP Accelerated is one example of how FedRAMP is making it easier for all providers to become FedRAMP compliant.
FedRAMP PMO should clarify if PaaS and SaaS providers can ride on a certified IaaS solution without having to get their own FedRAMP certification.	All cloud providers that hold Federal information must have a FedRAMP authorization. This clarification is in the Guide to Understanding FedRAMP, is listed in the FAQ's on FedRAMP.gov and has also been answered in the weekly FedRAMP tips and cues.
FedRAMP PMO should clarify and validate approved change management procedures.	Change management processes are defined through CSPs in their configuration management plan and the entire CM family of security controls in the FedRAMP baseline. Additionally, FedRAMP has defined processes for significant changes in the FedRAMP continuous monitoring strategy and guide as well as through the significant change impact analysis form on FedRAMP.gov.

RECOMMENDATION SIX: Establish Defense Department Crosswalk

Problem Statement	FedRAMP Response
Industry lacks clear information on the Defense Department's security control requirements and how they map to the FedRAMP High baseline.	This is something that DOD should work on – and they are continuing to update the security requirements guide. Additionally, DOD does have a gap analysis process for CSPs to get an authorization at DOD.
Recommended Actions	**FedRAMP Response**
Create and publish a taxonomy that clearly maps the controls included in FedRAMP Moderate in the context of other assessment levels, particularly DOD High.	DOD has published this and is available through DISA.
Institute a gap analysis process rather than forcing CSPs to start over again for DOD requirements.	This is exactly the process that DOD does with FedRAMP.