

## FedRAMP Accelerates the Process for Federal Contractors to Obtain Cloud Service Provider Authorizations and DoD Revises its Cloud Computing Security Requirements Guide for FedRAMP+

By C. Joël Van Over, Brian P. Cruz and Selena Brady

*Cloud computing is ubiquitous in the federal market place. Many federal contractors either provide cloud computing services to the government or use cloud computing services when performing a federal contract. For cloud service providers that wish to do business with the Federal government, it is a time of landmark changes.*

As a threshold requirement, a cloud service provider (CSP) must successfully navigate the Federal Risk and Authorization Management Program (FedRAMP) before it is authorized to provide a cloud service offering to the Federal government. The new FedRAMP Accelerated program, launched in March 2016, is intended to provide a faster, cost-effective, risk-based approach for authorizing CSP to provide cloud services to government agencies. FedRAMP is mandatory for low and moderate risk levels for all cloud deployments and associated service models. FedRAMP is currently developing a higher risk level authorization and has issued higher level certifications in a pilot program. CSPs that have not been certified by FedRAMP previously and either wish to provide cloud services to the federal government, or use cloud services in performing federal contracts, should consider the new FedRAMP Accelerated process to achieve the authority to operate in compliance with FedRAMP security control standards. This Advisory reviews the new FedRAMP Accelerated process, and provides background on FedRAMP for those considering the benefits of navigating the FedRAMP process. The General Services Administration (GSA) anticipates that the new accelerated process will reduce the time it takes to earn FedRAMP authorization by 75%, making it possible to achieve authorization in as little as three months.<sup>1</sup>

 <sup>1</sup> See [GSA Blog, FedRAMP Accelerated Announcement](#).

Also in March 2016, the Department of Defense (DoD) updated its Cloud Computing Security Requirements Guide (SRG), a significant document that establishes DoD's baseline security for cloud computing, effectively establishing FedRAMP+ requirements for DoD CSPs. Between March and June 8, 2016, DoD (through the Defense Information Systems Agency (DISA) has issued over 20 related Security Technical Implementation Guides (STIGS) that apply to specific technologies, products, and applications. The SRG requires compliance with all STIGs applicable to relevant systems.<sup>2</sup> According to DISA, "the STIGS contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious attack."<sup>3</sup> The SRG covers both internal DoD systems and external (commercial) CSPs and their cloud service offerings through the secret level security classification. DoD contractors are required to comply with the SRG under DoD's recently adopted cloud services regulations and implementing contract clauses.<sup>4</sup> The SRG describes how the FedRAMP process relates to SRG compliance and how it differs.

Both FedRAMP and the SRG are based upon National Institute of Standards and Technology (NIST) SP 800-53 Rev. 4 (2013) (Security and Privacy Controls for Federal Information Systems and Organizations), although the SRG also implements NIST SP 800-37 (2010) (Guide for Applying the Risk Management Framework to Federal Information Systems).<sup>5</sup> Both FedRAMP and the SRG use the broad NIST definition of Cloud Computing (NIST SP 800-145 (2011)).<sup>6</sup>

This Advisory reviews the new FedRAMP Accelerated process, and summarizes the relevance of FedRAMP to DoD contractors required to comply with SRG requirements under DFARS 252.239-7010, or through other tailored contract clauses.

## FedRAMP Background

Cloud services represent an increasing portion of government agencies' information technology \$80B spend from 2014-2016, and as the demand for cloud services increases, the government's concern for cybersecurity has also increased. To ensure that CSPs adopt baseline security measures to reduce security vulnerabilities, government agencies must require that CSPs possess FedRAMP authorization before performance of any cloud services contracts requiring low or moderate risk levels of protection.<sup>7</sup> The FedRAMP review and authorization process is rigorous and time-consuming. In an effort to balance the increased demand for cloud services and not negatively impact the quality of security, FedRAMP has introduced a new initiative, FedRAMP Accelerated. The changes under FedRAMP Accelerated are intended to achieve shorter timeframes for CSPs to achieve authorization as FedRAMP compliant. Although each agency remains responsible for determining the compliance of its cloud services contractors, the FedRAMP Accelerated process is intended to streamline the review by each agency for

<sup>2</sup> See SRG at § 1.4.

<sup>3</sup> <http://iase.disa.mil/stigs/Pages/index.aspx>

<sup>4</sup> See Defense Federal Acquisition Regulation Supplement (DFARS) Cloud Computing subpart 239.76, and the companion contract clauses, 252.239-7009 (Sept. 2015) and 239-7010 (Aug. 2015).

<sup>5</sup> See DoD Instructions 8500.01 (March 14, 2014), 8510.01 (March 12, 2014, change 1 May 24, 2016), and 8000.01 (March 17, 2016). See also NIST 800-146 (May 2012) (Cloud Computing Synopsis and Recommendations). Given the prominence of NIST standards in the cybersecurity arena, we recommend being aware of NIST publications and standards for cloud computing. See e.g. NIST SP 500-293 Vol. I and Vol. II (U.S. Government Cloud Computing Roadmap); NIST SP 500-291, Version 2 (NIST Cloud Computing Standards Roadmap); NIST SP 500-317 March 16, 2016 Draft (Cloud Computing and Accessibility Considerations); NIST SP 800-146 (Cloud Computing Synopsis and Recommendations); NIST SP 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems); NIST SP 800-53 Version 4 (Security and Privacy Controls for Federal Information Systems and Organizations). Note that NIST is in the process of developing Version 5 of NIST SP 800-53.

<sup>6</sup> NIST SP 800-145 (Definition of Cloud Computing).

<sup>7</sup> Private cloud deployments intended for single organizations and implemented fully within federal facilities are the only exception.

FedRAMP applicants. FedRAMP is a collaboration by the Department of Homeland Security (DHS), DoD, GSA, NIST, National Security Agency, Office of Management and Budget, the Federal Chief Information Officer Council and working groups to assist government agencies in meeting Federal Information Security Management Act (FISMA) requirements for cloud systems.<sup>8</sup> FedRAMP is governed by a Joint Authorization Board (JAB) comprised of the Chief Information Officers from the DHS, GSA and the DoD. FedRAMP provides a standard approach to security assessment, authorization and monitoring of cloud services for authorized security levels.<sup>9</sup> Initially launched in 2012, FedRAMP has issued authorizations to over 50 FedRAMP compliant CSPs.<sup>10</sup>

### Obtaining FedRAMP Certification

There are currently two potential paths for a CSP to gain authorization to provide cloud service offerings to federal agencies. Under either path, a CSP cannot provide a cloud service offering (CSO) to a particular agency until that agency has issued an Authority to Operate (ATO) at the appropriate security level. The CSP may pursue an ATO for a particular agency, or it may pursue a provisional ATO (P-ATO) through the JAB, which then permits the CSP to apply for an ATO with any agency at the security level authorized, or to proceed through an agency process for a higher level security ATO. A P-ATO is effectively the FedRAMP certification confirming that the CSP has a cloud service which is secure at the authorized security level and that an agency may issue an ATO to purchase the covered cloud service. Because each agency must issue its own ATO for a CSP, a P-ATO or an agency ATO is extremely valuable because it allows other government agencies to leverage the initial P-ATO or ATO without having to conduct a complete FedRAMP review process. Selecting the path a CSP will follow to become part of an official FedRAMP repository (accessible to all federal agencies) and obtain an ATO depends on whether a CSP seeks to offer government-wide cloud services, which requires undergoing a JAB review, or instead intends to target a single government agency, navigating the agency-specific approval process.

The FedRAMP Project Management Office (PMO) JAB review requires CSPs to submit documentation to the FedRAMP PMO and to the JAB and to undergo a complete security assessment where it is determined whether the CSP meets standardized requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations. The security assessment is performed by a FedRAMP accredited Third Party Assessment Organization (3PAO), engaged directly by the CSP. If the security controls and system are deemed appropriate, the JAB issues a P-ATO. The JAB is considered provisional because each agency must individually examine the CSP and determine whether to issue an ATO, assuming the risk of using the CSP. Generally, after obtaining the JAB P-ATO, government agencies purchasing cloud services from a CSP leverage the P-ATO to issue its own ATO.<sup>11</sup>

The alternate agency-specific review allows the CSP to submit its documentation and security package to a specific agency and the FedRAMP PMO. The CSP still undergoes a security assessment review for compliance with NIST 800-53, but the CSP may use an agency validated independent assessor, usually referred to as a 3PAO, although the 3PAO contracts directly with the agency, and not with the CSP. Payment to the 3PAO for its assessment service is a matter of contract administration. Once the CSP's system is deemed compliant, the specific sponsoring agency grants an ATO. Other agencies can then leverage the this ATO by reviewing the documentation and security package in the FedRAMP repository and issuing their own ATO based on the sponsoring agency's work and any additional security

<sup>8</sup> FISMA requirements are contained in 44 U.S.C. § 3531, et seq.

<sup>9</sup> See [GSA, FedRAMP Program Overview](#).

<sup>10</sup> See [GSA, FedRAMP Compliant Systems](#).

<sup>11</sup> See [Guide to Understanding FedRAMP, V2.0 at 16](#).

requirements imposed for various security levels.<sup>12</sup> FedRAMP discourages the agency level process now that FedRAMP Accelerated has been adopted.

### FedRAMP Accelerated

On March 28, 2016, FedRAMP Director Matthew Goodrich announced FedRAMP Accelerated, with the goal of CSPs obtaining a FedRAMP approval within three to six months, a significant reduction as current estimates for FedRAMP approval range from nine and eighteen months. FedRAMP Accelerated requires CSPs that intend to seek a JAB P-ATO to have a FedRAMP accredited 3PAO conduct an initial capabilities or “readiness” assessment before the JAB will review detailed documentation.<sup>13</sup>

The draft FedRAMP Readiness Assessment Guidance, released with the March 28 announcement, details 12 areas of readiness capability that the 3PAO reviews and assesses: access control, audit and accountability, configuration management, contingency planning/disaster recovery, identification and authentication, incident response, media protection, personnel security/credentialing, physical and environmental, risk assessment, system and information integrity and systems and communication protection.<sup>14</sup> A key aspect to FedRAMP Accelerated is the 3PAO’s Readiness Assessment Report, which details and describes the 3PAO’s review of the above areas. The draft Readiness Assessment Report was also released when FedRAMP Accelerated was announced.<sup>15</sup> The final versions of the Assessment Guidance and the Assessment Report are expected in June 2016. The Assessment Guidance provides that the 3PAO assessing FedRAMP readiness must provide a security capabilities rating for each readiness capabilities area and an overall security capabilities rating from Level I through Level V. The FedRAMP Security Assessment Framework, Version 2.1 (issued December 4, 2015) remains a useful guide.

If the CSP participating in the FedRAMP Readiness process obtains suitable ratings from the 3PAO, and the PMO agrees, then the CSP will receive a “FedRAMP Ready” designation and FedRAMP Ready documentation will be placed in a repository accessible to all federal agencies. FedRAMP anticipates that the FedRAMP Ready designation may lessen the value of the FedRAMP issued P-ATO, since agencies may more efficiently move directly to their own security assessment and issue an ATO. To achieve a P-ATO after the FedRAMP Ready designation, a full security assessment will be conducted and reviewed by the JAB and prioritized for authorizations with the JAB. Obtaining a FedRAMP Ready designation may be significant since government contractors may respond to a solicitation for a contract requiring an agency ATO, prior to obtaining an ATO. Already possessing an agency ATO, a P-ATO or a FedRAMP Readiness designation are advantageous discriminators. In the future, some agencies may even require a FedRAMP Readiness designation as a minimum prerequisite to submitting a proposal.

Although the Readiness Capabilities Assessment and the FedRAMP Ready designation are a prerequisite to the JAB approval for a P-ATO, there is no requirement that an individual government agency use or rely on the Readiness Capabilities Assessment when issuing agency ATOs. However, whether or not an individual agency has heightened security requirements, often referred to as “FedRAMP+”, it is highly likely

<sup>12</sup> See *id.*

<sup>13</sup> See [GSA, FedRAMP Accelerated Webinar](#).

<sup>14</sup> See GSA, Draft Readiness Capabilities Guidance for CSPs and 3PAOs, and the [FedRAMP Readiness Assessment Report](#).

<sup>15</sup> See *id.*

that the FedRAMP Ready designation will be leveraged as a baseline, and will result in a more efficient process for the issuance of agency ATOs.<sup>16</sup>

FedRAMP Accelerated is a substantive effort to streamline the FedRAMP authorization process. However, the new process requires substantial contractor advance work. The contractor-retained 3PAO must essentially audit the contractor's system, assist the contractor in correcting deficiencies, and document all elements required by the FedRAMP Readiness Assessment. The FedRAMP Security Assessment Framework and System Security Plan Templates are robust. FedRAMP has published numerous new subject specific templates in May 2016 in draft form that will be part of the required security assessment and documentation performed by an assessing 3PAO to achieve a FedRAMP Ready designation. Significantly, one of the new templates is a High System Security Plan High Baseline Template that covers controlled unclassified information. The low and moderate level security plan templates were updated earlier, after NIST issued Revision 4 to SP 800-53. While the contractor may assist in providing documentation and information required by the security plans templates, the templates require that the 3PAO preparing the plans be listed in the plan. The preparing 3PAO uses the appropriate security level plan for assessment and testing and documents actions and assessments in the Inventory Workbook Template, a key document in the authorization package submitted to FedRAMP. In sum, while FedRAMP Accelerated may streamline the FedRAMP process from a FedRAMP perspective, it remains unclear whether it will streamline the process overall.

### Initial Feedback Regarding FedRAMP Accelerated

GSA accepted comments on the Readiness Capabilities Report and Readiness Capabilities Guidance for CSPs and 3PAOs until April 29, 2016. On April 18, 2016, GSA released some of the initial responses from the comments and internal feedback from the current pilot participants for FedRAMP Accelerated. The comments process suggests that further FedRAMP guidance and possible amendments to draft templates may be issued in the near future. The feedback from comments revolved around the following issues:

- **The Evidence Necessary to Support the Readiness Assessment Report:** The PMO explained that CSP provided documentation cannot constitute the sole evidence to support the Readiness Assessment Report. The PMO's expectation is that 3PAOs will perform physical examinations, including an on-site visit, observations, evidence reviews, assessments of the trustworthiness of evidence, and personnel interviews in support of completing the FedRAMP Readiness Assessment Report.
- **Further Details Regarding the Capability Level Criteria:** Additional guidance was requested regarding the capability levels, whether certain capabilities have a minimum acceptable threshold, and which capabilities require a 3PAO's judgment given each CSP's system's requirements. Additionally, feedback was requested regarding interpreting the capability levels, as some are not intuitive given the FedRAMP requirements.
- **Additional Guidance for Rationale behind 3PAO Decisions:** Because the PMO wants to review the rationale behind the 3PAO's decisions, 3PAOs requested further guidance explaining what is required in the rationale.
- **3PAO Conflict of Interest:** Clarifications were requested for conflict of interest concerns, including whether a 3PAO can perform both a Readiness Capabilities Assessment and a full security assessment. In the GSA Weekly Tips on the FedRAMP website, the GSA provided clarification stating that the same

<sup>16</sup> *Id.*

3PAO can perform both the Readiness Capabilities Assessment and the security assessment for the new JAB P-ATO process without a conflict of interest. The 3PAO, however, cannot provide any consulting duties for the same authorization package.<sup>17</sup>

- **Determination of 3PAO's Overall Grade:** 3PAOs have concerns regarding the Readiness Capabilities Guidance document not specifying the method 3PAOs should use for selecting Level I through V value for the CSP's overall system. GSA has stated that it intends to respond to this issue.<sup>18</sup>

The PMO expects to finalize the FedRAMP Accelerated requirements by the end of June. We will update this Advisory when requirements, guidance, and templates become final. (Our other recent advisories on [continuing changes in cybersecurity regulations](#) and a [new cybersecurity regime to mandate secure information systems](#) provide further information on requirements and changes in the statutory and regulatory cybersecurity framework for Federal contractors.)

### **FedRAMP and The Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 2, March 18, 2016**

Under the recently adopted DoD cloud computing contract clause, DFARS 252.239-7010, DoD contractors and subcontractors “using cloud computing to provide information technology services in the performance of” a DoD contract must “implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG)”. The newly updated SRG, issued under the authority of DoD Directive 8500.01 and DoD Instruction 8510.01, implements NIST SP 800-37 and 800-53, the DoD Risk Management Framework, and the DoD associated cybersecurity policy.<sup>19</sup> The SRG applies to all CSP cloud services offerings (CSOs) and focuses on the service offerings, not the company IT system itself.<sup>20</sup> The SRG and numerous associated STIGs collect security requirements applicable to specific technology families, product categories or organizations generally.<sup>21</sup>

DoD employs FedRAMP as well as the SRG for cloud computing.<sup>22</sup> DoD issues a P-ATO or ATO based upon demonstrated compliance with FedRAMP and the additional security requirements that apply through the SRG at the applicable security level.<sup>23</sup> A CSP must have a DoD P-ATO or ATO, as specified by the SRG, for the CSOs it will provide. An offeror that does not hold a DoD P-ATO at the security level required by a solicitation must submit all FedRAMP documents and required DoD documentation with its response to the solicitation.<sup>24</sup> A DoD P-ATO and a mission owner ATO are required before a contract service goes into production with DoD data.<sup>25</sup>

Currently DoD accepts an agency ATO or a FedRAMP JAB P-ATOs through level 2, if the assessing 3PAO is an accredited FedRAMP 3PAO.<sup>26</sup> FedRAMP is implementing a higher level P-ATO, which may be leveraged by DoD, although additional requirements will apply since the SRG focuses on CSO risks, and

<sup>17</sup> See [GSA Weekly Tips](#).

<sup>18</sup> See GSA, FedRAMP Newsroom April 18, 2016 [Initial Readiness Assessment Report Feedback](#).

<sup>19</sup> SRG at § 1.2.

<sup>20</sup> *Id.* at § 1.3.

<sup>21</sup> *Id.* at § 1.4.

<sup>22</sup> *Id.* at § 1.

<sup>23</sup> *Id.* at § 4.3.1.

<sup>24</sup> *Id.* at § 4.5

<sup>25</sup> *Id.*

<sup>26</sup> *Id.* at § 2.4.

compliance with applicable STIGS is mandatory. At level 4 and above, security requirements become even more rigorous, as DoD assesses the impact of permitting the CSP to connect to DoD networks.<sup>27</sup> Strong virtual separation controls and monitoring are required at Level 4.<sup>28</sup> The risk assessment is based upon the DoD and NIST Risk Management Framework, as DoD transitions from the DoD Information Assurance Certification and Accreditation Process (DIACAP). Level 5 is reserved for DoD private/community clouds and many additional requirements apply.<sup>29</sup> Level 6 is related to systems authorized to hold classified information and are subject to additional requirements above those in the SRG.<sup>30</sup> All DoD security levels require ongoing assessments and continuous monitoring and this is often required to move from a P-ATO to an ATO for a particular CSO. DoD's focus is on mission risk.<sup>31</sup>

In sum, while DoD requires mandatory FedRAMP compliance and a JAB FedRAMP P-ATO or a FedRAMP agency ATO, DoD issues its P-ATOs and ATOs under heightened SRG requirements, especially when security above the FedRAMP moderate level P-ATO is required. As FedRAMP implements its higher level security P-ATO, it is likely that DoD will leverage such a P-ATO in the future. DoD has issued over 23 ATOs for FedRAMP moderate baseline CSOs that host non-controlled unclassified information.

## Conclusion

Ultimately, when a P-ATO or agency ATO is issued, the CSP will be held to the standards of the baseline requirements required for issuance of the authorizations. If there is a security breach, the Federal government conducts an investigation. It is prudent for the CSO to do the same, engaging counsel to protect confidentiality associated with the attorney-client privilege. Retained counsel will work with in-house IT and will likely recommend that counsel retain an independent expert to assist in the internal investigation. Because of the high risks associated with cyber incidents, and the requirements to report such incidents, acting quickly and systematically is necessary to mitigate risks.


---

If you have any questions about the content of this Alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

C. Joël Van Over **(bio)**  
Northern Virginia  
+1.703.770.7604  
joel.vanover@pillsburylaw.com

Brian P. Cruz **(bio)**  
Los Angeles  
+1.213.488.7101  
brian.cruz@pillsburylaw.com

Selena Brady **(bio)**  
Northern Virginia  
+1.703.770.7520  
selena.brady@pillsburylaw.com

 <sup>27</sup> *Id.* at § 4.3.2.

<sup>28</sup> *Id.* at § 5.2.1-2.

<sup>29</sup> *Id.* at § 5.2.2.3.

<sup>30</sup> *Id.* at § 5.2.2.4.

<sup>31</sup> *Id.* at § 4.3.3

**Pillsbury Winthrop Shaw Pittman LLP** is a leading international law firm with offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2016 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.