R311 - Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)

October 22, 2018

R311 – Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)

Table of Contents

Introduction

I. Scope

This document describes the requirements for Third Party Assessment Organizations (3PAOs) seeking A2LA accreditation in the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services.

All 3PAOs seeking accreditation under FedRAMP must meet the general requirements of ISO/IEC 17020:2012.

3PAOs seeking accreditation under FedRAMP through A2LA must also meet A2LA policy and requirements documents listed below.

A 3PAO which also has an affiliated testing laboratory in information technology may apply for accreditation for its testing laboratory concurrently with its application for accreditation for FedRAMP.

II. References

- *R102f – Conditions for FedRAMP Accreditation.*
- *R105 – Requirements When Making Reference to A2LA Accredited Status.*
- *R301 – General Requirements: Accreditation of ISO/IEC 17020 Inspection Bodies.*
- *R346 – Baltimore Cyber Range Technical Proficiency Testing Activity Information*
- National Institute of Standards and Technology (NIST) Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* December 2014. Available here: http://dx.doi.org/10.6028/NIST.SP.800-53Ar4
- *FedRAMP Security Assessment Framework (SAF).*
- *FedRAMP System Security Plan (SSP) Template.*
- *FedRAMP System Assessment Plan (SAP) Template.*
- *FedRAMP System Assessment Report (SAR) Template.*
- *FedRAMP Moderate Readiness Assessment Report (RAR) Template.*
- *FedRAMP High Readiness Assessment Report (RAR) Template.*
- *FedRAMP 3PAO Roles and Responsibilities.*
- *FedRAMP 3PAO Obligations and Performance Guide.*
- *FedRAMP Readiness Assessment – A Guide for 3PAOs.*
- *FedRAMP General Document Acceptance Criteria.*
- *FedRAMP Authorization Boundary Guidance.*
- *FedRAMP Penetration Test Guidance.*

III. Definitions

3.1 For the purposes of these requirements, the relevant terms and definitions given in ISO/IEC 17000, ISO/IEC 17020, and ISO/IEC Guide 2 apply. As used herein, the following terms shall have the meanings specified

3.2 3PAO personnel referred to in the following sections include full time, part time and contracted (i.e. 1099 contracts) individuals. All categories of personnel are expected to work within the parameters of the management system, be included

in witnessing activities and participate in the technical proficiency activity. All records of management system and technical training, along with records of witnessing and technical proficiency shall be maintained.

IV. General Requirements

4.1 Applicant and accredited organizations under this program consent to permit A2LA to provide assessment documentation (i.e., assessor reports, checklists, etc.), corrective action plans, and any associated objective evidence of resolution of deficiencies (where applicable) to the FedRAMP Program Management Office (PMO) upon request.

4.2 The organizational chart must clearly show the functions and lines of authority for staff within the applicant's organization and the relationship, if any, between the FedRAMP security assessment functions and other activities of the applicant's organization.

4.3 3PAOs must maintain a current list of customers, which shall include all FedRAMP assessment clients. If the 3PAO is part of an organization that offers consulting services to cloud service providers (CSPs), the 3PAO must maintain a customer list for both consulting services and FedRAMP assessment services. The customer list must include all customers from the previous three years. 3PAOs must provide a copy of this list to A2LA during all annual review and renewal assessments.

4.4 To proceed with the FedRAMP PMO recognition process, the organization must be accredited to ISO/IEC 17020 under the A2LA Cybersecurity Inspection Body Program for a period of one year as evidence of implementation of the required management system.

4.5 The 3PAO must meet the requirements for the technical proficiency activity as set forth in *R346 – Baltimore Cyber Range Technical Proficiency Testing Activity Information.*

4.6 As part of a renewal application, if a 3PAO is a Type C organization and provides consulting and/ or other cloud services for FISMA and/ or FedRAMP, the associated records may be requested as evidence of the 3PAO's understanding of the cloud consulting work. A2LA will use the evidence to help evaluate the 3PAO's understanding of FedRAMP in order to ensure the consulting services align with FedRAMP requirements. If it is determined by A2LA and/or the FedRAMP PMO that the evidence requested for the 3PAO cloud consulting work does not address FedRAMP requirements, this evidence may be grounds for revoking FedRAMP recognition.

4.7 During the on-site assessment, the assigned A2LA assessor will ensure there is a F337 - After Action Report completed for each assessment and the corresponding corrective actions have been recorded within the quality management system (QMS).

V. General 3PAO Requirements

5.1 The 3PAO must accommodate assessments by A2LA and/or the FedRAMP PMO when requested. "For cause" assessments are required to occur within ten business days from initial notification.

5.2 3PAO personnel participating in the FedRAMP Program must individually attest to their knowledge, understanding, and proficiency of the NIST Risk Management Framework, NIST 800-53 security controls, and FedRAMP security requirements and policies. This attestation will be captured in the *R102f – Conditions for FedRAMP Accreditation*. A2LA will assess all 3PAO candidates on this knowledge, understanding, and proficiency at the time of the on-site assessment. The resulting artifacts (including but not limited to, the A2LA assessment package provided after each assessment) are validated and verified by the FedRAMP PMO.

5.3 A2LA accreditation is the first step in gaining FedRAMP recognition. A2LA provides evidence to the FedRAMP PMO, but that does not imply acceptance to the FedRAMP program. A2LA submits the entire 3PAO assessment package (including the assessor report, corrective actions, correspondences and any Accreditation Council comments) to the FedRAMP PMO for final recognition. A 3PAO is not recognized by FedRAMP until the 3PAO receives an official recognition letter signed by the FedRAMP Director and is listed publicly on www.FedRAMP.gov.

5.4 The 3PAO must not submit any actual client records (i.e., SSP, SAP, SAR, etc.) to A2LA. These documents may be reviewed during the on-site assessment, but all confidential information must remain with the 3PAO.

5.5 To ensure there are no conflicts of interest between consulting and assessing, the FedRAMP PMO reserves the right to request customer records, policies, procedures, training records, and other similar records for FedRAMP consulting services of 3PAOs who are Type C organizations. Failure to provide these records can be grounds for revoking FedRAMP recognition.

VI. ISO/IEC 17020 Additional Requirements

Additional specific requirements for this program approved by the A2LA Criteria Council are described below. The numbering system for each section below corresponds to the major sections of ISO/IEC 17020. If a section is not listed below, there are no program specific requirements in addition to what is already stated in ISO/IEC 17020.

4.1-Impartiality and Independence

4.1.3 F.1 3PAOs must ensure they do not pose a risk to their impartiality in assessing systems that will potentially house U.S. Federal information. 3PAOs must ensure that all ownership, governance, personnel, finances, and payments for work align with all U.S. laws, policies, and regulations.

4.1.4 F.1 If a 3PAO has non U.S.-based personnel or OCONUS (outside of the continental United States) operations, the 3PAO must detail how the risk is minimized or eliminated.

4.1.6 F.1 The 3PAO must meet the requirements of either a Type A or Type C Inspection Body as defined in ISO/IEC 17020:2012. Type B Inspection Bodies are not permitted.

4.1.6 F.2 If a 3PAO is a Type C Inspection Body, the quality of all deliverables (from both assessment and consulting services) must meet all FedRAMP quality standards as defined through the FedRAMP General Document Acceptance Criteria on www.FedRAMP.gov. Deficiencies in meeting these quality requirements may be grounds for revoking FedRAMP recognition.

5.1-Administrative Requirements

5.1.4 F.1 The 3PAO must maintain appropriate insurance commensurate with the types of systems they provide assessments for and must disclose to A2LA what insurance policies they currently maintain.

5.2-Organization and Management

5.2.3 F.1 All assessments must be staffed by an appropriate number of team members based on the complexity of the cloud system being assessed. The number of team members must minimally consist of at least three people from the 3PAO, which includes, but is not limited to, 3PAO personnel types as defined in 6.1.1 F.1. The team, as a whole, is responsible for manual control testing, penetration testing, scanning, interviews, examination of artifacts, and report writing. During the A2LA onsite assessment, the 3PAO must demonstrate the ability to meet the team staff requirements.

5.2.4 F.1 If a 3PAO is part of an organization that offers consulting services to CSPs, the 3PAO is not permitted to inspect a CSP system that it has provided consulting services on within the previous two years.

5.2.4 F.2 If the 3PAO is part of an organization that is also a CSP, the 3PAO is not permitted to inspect the work of their organization's CSP.

6.1-Personnel

6.1.1 F.1 The 3PAO must define the types of personnel that perform assessments activities. Each personnel type must have defined competence requirements including education, training, technical knowledge, skills and experience. These requirements should be evidenced in a resume (or equivalent means) to demonstrate the fulfillment of the defined competencies below.

6.1.1.F.2 3PAOs must have a personnel type that is considered a "senior representative" who has the ability to sign off on assessments for the 3PAO. A senior representative must have at least five years of auditing and/or assessment experience and a minimum of two industry cybersecurity certifications (such as SANS GIAC, ISC2 CISSP, etc).

6.1.1.F.3 3PAOs must have a personnel type that is a "penetration tester" who has the technical competence to be able to complete a penetration test in accordance with FedRAMP Penetration Test Guidance and requirements. A 3PAO

penetration tester must have one year of penetration testing experience as the lead penetration tester, OR have at least one industry certification related directly to penetration testing (such as SANS GIAC Penetration Tester (GPEN) or OWASP Penetration Tester) and at least one other industry standard cybersecurity certification. Please note that the penetration testing certification that is held by the penetration tester should include hands-on (performance-based) components required for certification.

6.1.1.F.4 3PAOs must have a personnel type that is a "quality representative" who supports the assessment activities and provides support for the quality management of the documentation.

6.1.2 F.1 A 3PAO must have at least one person employed (not contracted or subcontracted) by the 3PAO for each personnel type identified in 6.1.1 F.1-4. Any 3PAO who does not have at least one person employed (not contracted or subcontracted) for each personnel type identified in 6.1.1 F.1-4, must be approved by the FedRAMP PMO prior to recognition of the 3PAO.

6.1.2 F.2 If a 3PAO has a large number of contract employees, 3PAOs must demonstrate that the contract employees have a continued and active relationship with the 3PAO and that they are active participants in the 3PAO QMS. The intention of this requirement is that a 3PAO must maintain the capability to perform a FedRAMP assessment while accredited.

6.1.5 F.1 The 3PAO must develop a training program for its personnel including, at a minimum, content incorporating FedRAMP, FISMA, cloud computing, and cybersecurity. This training program can include industry standard certifications or 3PAO developed training content. The 3PAOs must maintain a list of all training courses planned for the year and a statement for each item on the list as to how the training is related to these knowledge areas. The training program will be analyzed to determine if there is sufficient technical training of assessors for understanding FedRAMP, FISMA, cloud computing, and cybersecurity.

6.1.5 F.2 All authorized 3PAO personnel must complete at least 40 hours of training annually under the training program detailed in 6.1.5 F.1. These training hours may be completed through other accreditation programs with the completion of Continuing Professional Education (CPEs) or equivalent, as long as it is defined adequately within 6.1.5 F.1, above. However, this 40 hours of training annually is in addition to training released by the FedRAMP PMO.

6.1.7 F.1 3PAO personnel must register for and then complete FedRAMP-sponsored 3PAO training modules and FedRAMP-provided program update sessions within 60 days of the training and/or update announcement. All new trainings will be announced to the 3PAO's POC on file with the FedRAMP PMO. At the close of the 60 day time period for completing each training module that is released, the 3PAO must provide copies of "certificates of completion" for all 3PAO personnel who participate in the FedRAMP Program to the FedRAMP PMO (info@fedramp.gov) and also maintain copies of these certificates in their training records. Records of completion will be reviewed during the on-site assessment to ensure each team member

has participated appropriately. Each individual 3PAO participant who has not completed the required trainings or update sessions may not participate in FedRAMP assessment activities until the proof of completion is sent to the FedRAMP PMO as detailed above. Any exceptions to this must be approved by the FedRAMP PMO.

6.1.10 F.1 The 3PAO must maintain training records for all their personnel (including subcontracted/1099 personnel) that have been involved with FedRAMP assessments for the past two years.

6.1.10 F.2 All training records shall list the name of the organization that provided the training, the date the training occurred, and the topic of the training course.

6.1.10 F.3 The 3PAO must create a 3PAO Technical Proficiency Activity Participation Plan to address when each member of the team participates in the hands-on technical exercise at least once every 12 months. 3PAO personnel must be included in the plan, and records including pass/fail ratings shall be maintained.

6.2-Facilities and Equipment

6.2.1 F.1 If a 3PAO does not have a commercial facility, the 3PAO must provide justification detailing the availability, suitability, and adequacy of the facilities, equipment and tools being used (including scanning equipment, laptops, licensing, and operational tools such as email, customer data tools, QMS materials etc.).

6.2.13.b F.1 The 3PAO's procedures for protecting and securing the integrity of data (ISO/IEC 17020:2012 clause 6.2.13b) must also address collection, transmission and storage of data collected by any contracted personnel that data shall be held secure by the contracted personnel until it is transferred to the 3PAO for final review and reporting.

6.3-Subcontracting

6.3.1 F.1 If a 3PAO subcontracts out any part of the assessment, it must ensure and be able to demonstrate that the subcontracted company is competent to perform the tasks and must comply with the relevant requirements and standards.

6.3.1 F.2 The subcontractor must be trained on the 3PAO's quality management system in order to ensure compliance with ISO/IEC 17020:2012. These trainingrecords must be maintained by the 3PAO.

6.3.1 F.3 All subcontractors must also meet the same position description requirements of similar positions within the 3PAO organization.

6.3.1 F.4 3PAOs should only subcontract as an exception to the normal course of business and should not regularly contract with clients beyond their capabilities and resources as described in ISO/IEC 17020:2012: Section 6.3 Subcontracting Note 1.

6.3.1 F.5 3PAOs must ensure that all subcontracted companies are available for any follow up actions required by FedRAMP or A2LA related to any assessment they worked on.

6.3.3 F.1 Whenever subcontracted companies perform part of the assessment, the responsibility for ensuring that all work is performed in conformance with A2LA and FedRAMP requirements must remain with the 3PAO.

6.3.3 F.2 If a 3PAO chooses to subcontract part of a FedRAMP engagement to another company, the requirements listed above can be waived if the subcontracted company is an accredited 3PAO.

7.1-Inspection Methods and Procedures

7.1.1 F.1 3PAOs must ensure that all 3PAO prescribed methods and procedures for a CSP system, align with most current NIST, DHS, and FedRAMP policies and procedures, and industry best security practices. In particular 3PAOs must comply with all FedRAMP policies and guidance documents publicly available on www.FedRAMP.gov.

7.1.5 F.1 During the contract review process, the CSP must be informed of their ability to proactively provide feedback on the 3PAO's performance directly to A2LA and the FedRAMP PMO at any time throughout the process. The *F338 – CSP Evaluation Form* is available on the A2LA portal and the A2LA public website (www.A2LA.org) and must be provided to the CSP once the work has begun.

7.1.5 F.2 At the completion of a FedRAMP assessment, a 3PAO must inform the CSP that FedRAMP may not post their authorization on www.FedRAMP.gov until the *F338 - CSP Evaluation Form* is provided by the CSP to the FedRAMP PMO (info@fedramp.gov) and A2LA (FedRAMP@A2LA.org).

7.4-Inspection Reports

7.4.1 F.1 3PAOs must have a documented quality review process for all FedRAMP deliverables.

7.4.2 F.1 All SARs written by the 3PAO must include an authorization recommendation on whether the system can appropriately safeguard government data in accordance with the security classification of the system. The recommendation shall include a summary statement and justification statement.

7.4.4 F.1 After each engagement (either readiness or full engagements), the 3PAO must create an After Action Report. The *F337 – After Action Report Form* is available on the A2LA portal and the A2LA public website (www.A2LA.org). The completed reports should be submitted to the FedRAMP PMO (info@fedramp.gov) and to A2LA (FedRAMP@A2LA.org) within 30 days of the end of the engagement. CSPs will not be listed as authorized or FedRAMP Ready on www.FedRAMP.gov until the 3PAO completes and submits the corresponding F337 form.

8.1-Options

8.1.1 F.1 As long as the 3PAO maintains accreditation, it must continue to implement its ISO/IEC 17020:2012 management system even if they are not working on any FedRAMP engagements.

8.1.3 F.1 All 3PAO applicants will be assessed on the management system requirements listed in Section 8, Option A of ISO/IEC 17020:2012.

8.7-Corrective actions

8.7.2 F.1 3PAOs should expect to receive feedback from the FedRAMP PMO after each assessment is reviewed. 3PAOs must review the feedback and, as necessary, utilize their corrective action and complaints process. Decisions related to the feedback may result in updates to 3PAO policies, procedures, and the management system.

REVISION HISTORY

DATE	REVISION
11/8/2013	Initial publication.
12/22/2016	Complete document re-write
03/13/2017	Removal of requirement that a 3PAO cannot assess a CSP that inherits or leverages a portion of its security requirements from a CSP the 3PAO has previously consulted on.
10/22/2018	Added additional document references to Section II. Defined 3PAO personnel, removed the term "key inspection body personnel". Removed referenced to the outdated Notional SSP process, added information on the Technical Proficiency Testing Activity. Clarified in Sections IV and V the qualification process for organizations to receive FedRAMP 3PAO recognition. Updated expectations on organizations who conduct international business. Added requirements for each defined personnel type required to participate in assessments. Clarified expectation of relationships of contract/1099 employees. Added requirement to complete at least 40 hours of training. Added requirement for creation of Technical Proficiency Activity Participation Plan. Added requirement for evidence of suitable facilities should the organization not have a physical office. Clarified requirements for subcontracted companies. Forms F337 and F338 are now required to be completed prior to authorization being granted. Added requirement for PMO feedback to be formally acknowledged through the management system.