Federal Risk and Authorization Management Program
General Services Administration
1800 F Street, NW, Washington, DC 20405
info@fedramp.gov | www.fedramp.gov

Date: December 19, 2024

TO: FedRAMP Recognized 3PAOs

FROM: Pete Waterman
FedRAMP Director

Re: Public Comment on Proposed Revisions to FedRAMP 3PAO Requirements

---

FedRAMP Recognized 3PAOs –

As a part of FedRAMP's ongoing commitment to improvement and stakeholder engagement, a 3PAO strategy session was held in FY24 to collaborate on solutions for addressing current challenges faced by both FedRAMP and FedRAMP recognized 3PAOs. Specifically, two main challenge areas were discussed:

1. FedRAMP highlighted the persistence of assessment deliverables that did not meet FedRAMP performance standards around documentation quality and testing accuracy/completeness, which resulted in multiple security package resubmissions.
2. The 3PAO participants expressed their concerns regarding the high costs of training junior staff, which was inhibiting team growth.

At the conclusion of the session, a consensus was made that the best approach to address these challenge areas was to revise FedRAMP's 3PAO requirements around training and certifications to minimize 3PAO personnel training costs while also ensuring assessors were sufficiently trained to produce high quality products to the federal government.

As a next step, FedRAMP worked with the American Association for Laboratory Accreditation (A2LA) to identify how to best revise FedRAMP's 3PAO policy (A2LA R311 – Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)), which is published, maintained, and enforced by A2LA. This collaboration resulted in the following general and personnel proposed requirement revisions (highlighted in yellow) organized by the section they appear in the current version of the A2LA R311:

General Requirements

1.) **Requirement 4.5**: Participation in the Baltimore Cyber Range (BCR) technical participation activity was expanded to include an individual testing exercise for penetration testers.

BCR Cyber Penetration Tester Technical Proficiency Activity

The BCR Cyber Penetration Tester Technical Proficiency Activity is an individual certification obtained by the penetration tester which consists of a multiple-choice written evaluation and a real-time assessment of a multi-server network environment. Both the written and network evaluation are conducted remotely with the penetration tester utilizing a third party assessment organization (3PAO) workstation for evaluation access.

The written evaluation provides the practitioners an opportunity to demonstrate basic penetration knowledge while the assessment exercise evaluates the practitioner's ability to perform a penetration test and identify issues of a compromised network. To assure fairness, practitioners are provided a common suite of industry standard tools. Note, the penetration tester must have sufficient knowledge of Kali Linux and Metasploit tools to perform the technical testing activities. Network external and internal Kali Linux/Metasploit servers are provided for practitioner use. The target system includes Windows workstations, Linux servers, Windows servers, and a pfSense router. The practitioner must map system component implementation and configuration issues to NIST SP 800-53A controls and/or control enhancements identified for each individual evaluation activity. Actual exam content varies per individual tester.

Five NIST SP 800-53A controls/control enhancements are presented for evaluation. The activity is intended to demonstrate a practitioner's ability to test and accurately identify evidence/artifacts required to document non-compliant security controls in the multi-server network environment. The provided Penetration Evaluation Test Report (PETR) template is the testing activity report document.

Participation Details

The evaluations are completed remotely. Zoom, a compatible browser, high-speed internet access, access to the assessors' email account, and a

workstation camera (to support Zoom) are the key system evaluation requirements. Access to the evaluation network is provided via browser. Required credentials are provided at the start of the evaluation.

Impact and Rationale: Currently, only senior and junior assessors are required to demonstrate their FedRAMP assessment competencies by taking and passing the BCR technical proficiency exercise. Penetration testers will now also be expected to take and pass a technical exercise focused on how to perform a penetration test based on FedRAMP standards. This will enable FedRAMP and 3PAOs to ensure penetration testers have the minimum qualifications needed to successfully perform a FedRAMP-specific penetration test.

Personnel Requirements

2.) **Requirement 6.1.1 F.2**: The senior assessor role's experience and certification levels were revised for closer alignment with the DoD 8140 Cyber Workforce Qualification Program certification requirements for training, certifying, and managing a cybersecurity workforce.

3PAOs must employ at least one "senior assessor" for each FedRAMP assessment, regardless of the type of assessment. This individual is accountable for the overall quality of deliverables and signs off on assessment activities performed by the rest of the team. A senior assessor must have at least five years of auditing and/or assessment experience and maintain at least two certifications, where at least one certification must be from the Tier 1 Certifications list (below) and an additional certification from either of the associated certification tiers (i.e., Tier 1 or Tier 2) annotated below:

A senior assessor must have at least five years of auditing and/or assessment experience and maintain at least two certifications, where at least one certification must be from the Tier 1 Certifications list (below) and an additional certification from either of the associated certification tiers (i.e., Tier 1 or Tier 2) annotated below:

Tier 1 Certifications

- *Certified Information Systems Security Professional or Associate (CISSP or Associate)*
- *CISSP-Information Systems Security Architecture Professional (CISSP-ISSAP)*
- *CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)*
- *CISSP-Information Systems Security Management Professional (CISSP-ISSMP)*

- *Certified Cloud Security Professional (CCSP)*
- *CompTIA Advanced Security Practitioner (CASP+)*
- *Certified Information Systems Auditor (CISA)*
- *Certified Information Security Manager (CISM)*
- *GIAC Certified Enterprise Defender (GCED)*
- *GIAC Certified Incident Handler (GCIH)*
- *GIAC Security Leadership (GSLC)*
- *CyberSec First Responder (CFR)*
- *Certified Chief Information Security Officer (CCISO)*

Tier 2 Certifications

- *Governance, Risk, and Compliance Certification (CGRC)*
- *AWS Certified Solutions Architect – Associate, Professional, or Security Specialty*
- *Azure Security Engineer Associate*
- *Google Professional Cloud Architect*
- *Oracle Cloud Infrastructure Architect*
- *GIAC Systems and Network Auditor (GSNA)*
- *GIAC Security Essentials (GSEC)*
- *CompTIA Cybersecurity Analyst (CySA+)*
- *CompTIA Cloud+ (Cloud+)*
- *CompTIA Security+ (Security+)*
- *Certificate of Cloud Security Knowledge (CCSK)*
- *Global Industrial Cyber Security Professional (GICSP)*

Impact and Rationale: 3PAOs indicated that it was critical for their organizations to align FedRAMP personnel certification requirements with other major government compliance programs to allow maximum flexibility for how they staff assessments.

3.) **Requirement 6.1.1 F.3:** The penetration tester role's experience and certification levels were revised for closer alignment with the DoD 8140 Cyber Workforce Qualification Program certification requirements for training, certifying, and managing a cybersecurity workforce.

3PAOs must have a personnel type that is a "penetration tester", for each FedRAMP assessment, that has the technical competence to perform a penetration test as part of the assessment scope. This individual must have the technical competence to be able to lead the penetration test, in accordance with FedRAMP Penetration Test Guidance and requirements. This person must also be proficient in planning, executing, and reporting on all facets of the penetration test. A 3PAO penetration tester must have two years of penetration testing experience and at least one industry certification related to enhancing the knowledge and skills needed to perform penetration testing activities from

the following list:

- *Cisco Certified Network Professional Security (CCNP Security)*
- *CompTIA Advanced Security Practitioner (CASP+) Continuing Education (CE)*
- *Certified Information Systems Security Professional (CISSP)*
- *Certified Secure Software Lifecycle Professional (CSSLP)*
- *CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)*
- *SANS GIAC Penetration Tester (GPEN)*
- *GIAC Certified Enterprise Defender (GCED)*
- *Certified Ethical Hacker (CEH)*
- *Cisco Certified Network Associate-Cyber-Ops (CCNA Cyber Ops)*
- *Computer Hacking Forensics Investigator (CHFI)*
- *GIAC Certified Forensic Analyst (GCFA)*
- *CompTIA PenTest+*
- *OffSec Certified Professional (OSCP)*
- *OffSec Web Expert (OSWE)*
- *OffSec Experienced Pentester (OSEP)*
- *OffSec Web Assessor (OSWA)*
- *Certified Professional Penetration Tester (eCPPT)*
- *Web Application Penetration Tester (eWPT)*
- *Web Application Penetration Tester eXtreme (eWPTX)*
- *Hack the Box Certified Penetration Testing Specialist (HTB CPTS)*
- *Burp Suite Certified Practitioner*

Impact and Rationale: 3PAOs indicated that it was critical for their organizations to align FedRAMP personnel certification requirements with other major government compliance programs to allow maximum flexibility for how they staff assessments.

4.) **Requirement 6.1.1 F.4:** The certification requirements for the junior assessor role were removed.

Impact and Rationale: 3PAOs indicated that a more cost effective approach to train their junior assessor personnel was for their organizations to develop a robust FedRAMP-specific organizational training program (see Appendix A below). Additionally, by not requiring specific certifications for their junior assessor staff, 3PAOs have more flexibility to hire junior level assessors and have them immediately support assessments under the supervision of their senior assessor leads.

5.) **Requirement 6.1.5 F.1:** 3PAO organizational training program requirements were further defined to include specific FedRAMP knowledge areas for all personnel who perform FedRAMP assessments. These specific FedRAMP knowledge areas are mentioned in Appendix A below.

> *3PAOs must develop an organizational training program for all its personnel (not only specific to the "senior assessor" and "penetration tester" roles) including content incorporating continuing professional education (CPE) credits for the FedRAMP knowledge areas specified in Appendix A. Training shall comprise a minimum of 6 hours for each of the FedRAMP knowledge areas mentioned in Appendix A. 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 plan must be based on the employee role in the assessment team and shall clearly delineate the intent of the plan for that individual role. The overall organizational training program will be analyzed to determine if there is sufficient technical training of assessors for understanding FedRAMP.*

Impact and Rationale: 3PAOs indicated that a more cost effective approach to train their junior assessor personnel is for their organizations to develop a robust FedRAMP-specific internal training program based on knowledge areas prescribed by FedRAMP. This training program will provide specific elements that FedRAMP requires 3PAO personnel to be trained on based on common issue areas found in 3PAO assessment deliverables and establishes a level of training consistency across all 3PAOs in the program.

6.) **Requirement 6.1.5 F.2:** The number required annual training hours for 3PAO personnel was reduced from 32 to 24 hours.

All authorized 3PAO personnel must complete at least 24 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 the hours are defined adequately within 6.1.5 F.1, above. The sign off on successful completion of the CPEs is required and records shall be maintained. Also, the 24 hours of training annually is in addition to the mandatory training released by FedRAMP.

Impact and Rationale: 3PAOs expressed concern that 32 hours of individual personnel training was overly burdensome for their organizations financially, especially for organizations with large teams, due to also being required to maintain personnel certifications and BCR proficiency training. As an alternative,

3PAOs will need to implement a more structured internal training program for all of their personnel that incorporates FedRAMP-specific knowledge areas as specified in Appendix A below.

7.) Appendix A FedRAMP Focus Areas for 3PAO Organizational Training Program: Four (4) FedRAMP focus areas were defined as a basis for the development of an internal 3PAO training program.

All personnel in the "senior assessor" or "junior assessor" role must receive focused internal training on four (4) FedRAMP focus areas:

1. FedRAMP authorization boundary, dataflow, and network diagrams
    a. FedRAMP Authorization Boundary Guidance
    b. Security controls relating to the authorization boundary, dataflow, and network diagrams (including all relevant security control enhancements) such as: AC-20, CA-3, CM-12, SA-9, SC-7, and SI-4
    c. Illustrating the essential elements of authorization boundary, dataflow, and network diagrams to include components such as subnets, alternate processing/storage sites, mobile applications, development/test environments, FIPS 140 validated encryption, and multi-factor authentication methods
2. FedRAMP FIPS 140-validated encryption
    a. NIST Cryptographic Module Validation Program (CMVP)
    b. FedRAMP SSP Template - Section 10
    c. FedRAMP SSP Template Appendix Q - Cryptographic Modules Table
    d. Security controls relating to encryption requirements (including all relevant security control enhancements) such as: AC-17, AC-18, AC-19, IA-5, MP-5, SC-7, SC-8, SC-13, and SC-28
    e. NIST SP 800-63-3 Digital Identity Guidelines
3. FedRAMP NIST SP 800-53 and 800-53A security control interpretation methods
    a. Understanding the differences between leveraged and inherited security controls in a CSP's SSP
    b. How to identify security controls that are applicable vs. not applicable in a CSP's SSP
    c. How security controls need to be documented in the CIS/CRM
    d. How to recognize errors concerning "Configuration Settings"
    e. How to differentiate between Control Implementation Summary (CIS) designations
    f. How to recognize inconsistencies among related security controls
    g. How to recognize effective policies and procedures for a given security control

h. How to determine if a security control adequately describes the who, what, when, where, why, and how in a SSP's implementation description
i. How to validate customer responsibilities (ensuring at least one option/solution required of a customer meets FedRAMP requirements)

4. FedRAMP multi-factor authentication requirements
    a. NIST Special Publication 800-63 (most current revision)
        i. Differences between the IAL1, IAL2, and IAL3 identity assurance levels
            - Importance of IAL information
            - Identity proofing user journey
            - IAL requirements summary
        ii. Differences between the AAL1, AAL2, AAL3 authentication assurance levels
            - Importance of AAL information
            - AAL2 permitted authenticator types, authenticator, and verifier requirements
            - AAL3 permitted authenticator types, authenticator, and verifier requirements
            - AAL requirements summary
        iii. Differences between the FAL1, FAL2, and FAL3 federated assurance levels
            - Importance of FAL information
            - Federation threats and attacks
            - Federation threat mitigation strategies
            - Security Assertion Markup Language (SAML), kerberos, OpenID connect/how they relate to the FAL paradigm
    b. FedRAMP security control baseline discussion (including all relevant control enhancements) such as: IA-2, IA-2(1), IA-2(2), IA-2(6), IA-5, and IA-8
    c. Overview of NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions
        i. Identity proofing
        ii. Authentication
        iii. Federation and assertions

All personnel in the "penetration tester" role must receive focused internal training on four (4) FedRAMP focus areas:

1. Vulnerability scanning versus penetration testing
    a. What is penetration testing?
        i. What is the scope of penetration testing?

   ii. Associated threat models applicable to a particular system
   iii. Penetration testing alignment with the FedRAMP security control baselines
      - Penetration testing in relationship to all FedRAMP baselines
      - Security controls associated with penetration testing exercises
  b. What is the scope of vulnerability scanning?

2. MITRE ATT&CK® Matrix for Enterprise
  a. What is the MITRE ATT&CK® Matrix for Enterprise?
    i. When is this used?
    ii. Why is this used?
    iii. How is this used?

3. FedRAMP mandatory attack vectors and applicability to a particular system
  a. Attack Vector 1: External to Corporate
  b. Attack Vector 2: External to CSP Target System
  c. Attack Vector 3: Tenant to CSP Management System
  d. Attack Vector 4: Tenant-to-Tenant
  e. Attack Vector 5: Mobile Application as part of Target system
  f. Attack Vector 6: Client-side Component as part of Target System

4. FedRAMP penetration testing reporting requirements
  a. Familiarity with penetration testing rules of engagement
  b. How are penetration testing deficiencies reported in a security assessment package?

Impact and Rationale: This internal training program will provide specific elements that FedRAMP requires 3PAO personnel to be trained on based on common issue areas found in 3PAO assessment deliverables and establishes a level of training consistency across all 3PAOs in the program.

If you have comments, edits, or feedback on the proposed A2LA R311 updates, please follow the instructions at https://fedramp.gov/updates/rfcs/0002/ to participate in public comment. Please also be sure to include the specific draft requirement number to which your question or comment refers.

As always, we appreciate your input. If you have any questions please email info@fedramp.gov.