FedRAMP Transport Layer Security (TLS) Requirements

Version 1.0

January 31, 2018

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
1/31/2018	1.0	All	Initial document	FedRAMP PMO

ABOUT THIS DOCUMENT

This document provides revised guidance and requirements related to the Transport Layer Security (TLS) protocol in support of achieving and maintaining a Federal Risk and Authorization Management Program (FedRAMP) security authorization. FedRAMP-authorized systems must be fully compliant **by July 1, 2018**.

This document is not a FedRAMP template – there is nothing to fill out in this document.

This document uses the term *authorizing official* (AO). For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says Agency AO. For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging Agency's AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by Cloud Service Providers (CSPs), Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP projects.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

1. PURPOSE

This document summarizes the National Institute of Standards and Technology (NIST) and Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01 requirements to implement current TLS protocols and restrict the use of older protocols.

This document establishes revised guidance and requirements for TLS, which FedRAMP CSPs must implement by July 1, 2018 for FedRAMP-authorized systems.

2. BACKGROUND

TLS is a set of cryptographic protocols that provide communications security over computer networks. *NIST Special Publication 800-52,* Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, required the use of TLS version 1.1 at a minimum and strongly recommended that "agencies develop migration plans to TLS version 1.2 by January 2015." The purpose of the NIST requirement to move to TLS 1.1, or higher, is to promote the "consistent use of recommended cipher suites that encompass NIST-approved algorithms" and to protect against known and anticipated attacks on the TLS 1.0 and SSL protocols.

3. TLS REQUIREMENTS

FedRAMP carefully reviewed the NIST and DHS requirements and determined that each FedRAMP-authorized system must fully implement TLS version 1.1 or higher. These requirements are only applicable to federal customers. However, if a CSP is not fully implementing NIST-compliant TLS for all customers, the CSP must be able to segment federal and non-federal customers prior to authenticating, thus ensuring federal customers use NIST-compliant TLS at all times. This means NIST-compliant TLS must be implemented prior to authenticating both federal and non-federal customers for all customers.

4. TRANSITION PLAN

These requirements are effective immediately, and each FedRAMP system must be fully compliant with the NIST TLS requirements **by July 1, 2018**.

By March 31, 2018, each CSP must provide written notification to the FedRAMP Program Management Office (PMO) identifying when their cloud service offering will be fully transitioned to use of TLS 1.1 or higher.

If the CSP anticipates being unable to meet the July 1, 2018 deadline, the written communication must also include a justification and a plan of action detailing how and when the CSP will achieve full transition to TLS 1.1 or higher. Where full implementation is not possible, the CSP must work with their AO on a mitigation plan. The AO must review and approve the CSP's implementation or mitigation plan.

For systems with a JAB P-ATO, the CSP should post the plan to OMB MAX and send an email notification to info@fedramp.gov, or discuss an alternative arrangement with their FedRAMP POC. For systems with an Agency AO, please coordinate with the AO's office for an appropriate delivery mechanism.

For systems with a JAB P-ATO, FedRAMP will track the TLS transition status as part of monthly continuous monitoring activities and include this status in the monthly ConMon Report. For systems with a FedRAMP Agency ATO, the CSP must consult with their Agency AOs regarding implementation status tracking. Agency AOs will likely require the CSP to track implementation via an entry to the system's Plan of Actions and Milestones (POA&M).

Guidance on TLS 1.1 implementation is provided in *NIST SP 800-52, Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementation*. Current guidance on authentication is provided in *NIST SP 800-63, Revision 3, Digital Identity Guidelines*, and *NIST SP 800-63B, Authentication and Lifecycle Management*.

Operating at TLS 1.1, or higher, will be a FedRAMP requirement moving forward; therefore any CSP not yet authorized should plan to address these requirements as part of their authorization activities.

APPENDIX A: FedRAMP ACRONYMS

The *FedRAMP Master Acronyms & Glossary* contains definitions for all FedRAMP publications, and is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.