

We are now FedRAMP Ready

**Partner with Verizon to enable
a centralized, standardized
security policy across your
entire network using Verizon
Government Cloud SD WAN**



The rapid adoption of cloud and mobile technologies requires your government agency to balance application performance, security and cost efficiency. Software-defined wide area network (SD WAN) solutions can help achieve this balance without compromise.

When you partner with Verizon, your agency can address these challenges and ensure that our cloud environment and SD WAN solution align closely with your mission requirements, compliance and security standards.

Partner with Verizon and move your agency forward

SD WAN brings powerful new features, but along with the many benefits comes additional complexity in security, Quality of Service (QoS), protocols, service types, devices, controllers and operating systems. And while you may want to adopt hybrid platforms, you may not have staff with the expertise to manage the risks that come with it.

**Our Government Cloud SD WAN
solution is FedRAMP Ready and
with your agency authorization, you
gain a cloud solution that meets the
customized needs of your mission.**

Sponsor your SD WAN service with Verizon

Your agency may require specialized expertise, tailored solutions or step-by-step assistance with FedRAMP compliance for your specific mission. By partnering with Verizon and our dedicated team of experts, you gain:

- More control over the environment and customization of the security posture, rather than relying on existing and previously authorized systems
- Alignment with your agency's specific security requirements, levels of data sensitivity and classifications, plus geographical and operational constraints
- A more flexible and scalable route towards implementing a solution that meets your agency's specific timelines and evolving mission requirements
- Access to Verizon's innovative technologies, services, capabilities, advanced security features and support
- Up-to-date infrastructure and security measures in alignment with the latest FedRAMP requirements
- Verizon's ownership and complete visibility over the cloud solution, including risk practices, ensuring the highest levels of accountability and responsibility
- Confidence that our SLA's, performance targets and support response times align with your specific needs
- A direct relationship with our experts to ensure proactive, continuous monitoring, timely updates and up-front communication when vulnerabilities and incidents arise
- Trust in your required compliance standards being met for regulations beyond FedRAMP including HIPAA, ITAR and more

verizon

Partner with Verizon through the agency authorization process

Upon receiving a written confirmation of the agency's intent to authorize the sponsorship process for Verizon FedRAMP High accreditation, there are activities Verizon, the 3rd party assessment organization (3PAO) and the agency would undertake.

The following steps for Verizon and a federal agency to take to meet the FedRAMP requirements for an Authority to Operate sponsorship related to the SD WAN solution. The path outlined below is based on FedRAMP PMO requirements for the FedRAMP High authorization process. The process typically takes 6-9 months.

1

Sponsorship/SD WAN project kickoff call

The agency, Verizon and the 3PAO would have a meeting of stakeholders to outline the overall FedRAMP sponsorship process, including roles and responsibilities.

Note: A representative of the FedRAMP PMO may be in attendance during this meeting.

- Overview of the Verizon Government Cloud hosting environment and the SD WAN solution, architecture, boundaries, data flows and security capabilities.
- Understand role of Verizon's 3rd Party Assessment Organization (3PAO) in the authorization process.
- Review of the Readiness Assessment Report (RAR), which documents the system information, federal compliance, and ability to meet FedRAMP security requirements.
- Explain the scope of the security assessment of Verizon's system with respect to the SD WAN environment.
- Schedule project meeting cadence

2

Security Assessment Review (SAR) of Verizon (4-6 months)

To provide clarity and visibility in the security posture of Verizon's SD WAN Govt Cloud solution, an independent assessment will occur of Verizon's SD WAN environment.

Note: The SAR is the basis for federal agencies to make security authorization decisions.

- 3PAO performs an independent Security Assessment Report (SAR) of Verizon's security parameters with respect to FedRAMP High level requirements.
- The SAR verifies the implementation of security controls and provides an overall risk posture of the Verizon service.
- 410 controls are required to be assessed of Verizon's environment for FedRAMP High level certification. This is a more stringent evaluation than the assessment to obtain FedRAMP High Ready State.

3

SAR debrief of Verizon's security posture

At this stage in the process, the SAR has been completed and will be shared with the agency for their review.

- The 3PAO findings (i.e. non-conformities, areas for improvement) are presented and remediation plans/timelines are developed.
- The agency conducts a quality and risk review to assess the accuracy and completeness of Verizon's 3PAO generated SAR and security posture

4

Agency determination of Verizon system activation within network

With the agency completing the SAR review and remediation timelines are met, activation can be performed.

- Upon the agency validating Verizon's SAR findings are addressed and meets both the agency and FedRAMP required protocols, the agency would develop the Authority to Operate (ATO) letter for the FedRAMP PMO

5

FedRAMP High authorization granted

Upon the receipt of the assessment and agency ATO letter, the FedRAMP team performs a review for full authorization.

- Once the FedRAMP PMO receives the audit and authorization package, they evaluate that the security parameters are met, Verizon would be granted full FedRAMP High authorization and the agency would be informed.
- FedRAMP PMO adds Verizon to the external marketplace for public visibility.

6

Continuous monitoring (annual)

Verizon is required to maintain their FedRAMP High Authorized SD WAN environment after achieving the authority to operate. This is performed by the 3PAO on an annual basis.

- Verizon, through internal evaluations, assesses their SD WAN environment on a regular basis to monitor their security control or identify network issues or anomalies.
- The agency would review the 3PAO continuous monitoring assessment and validate its conclusions.
- Agency validation provided to the FedRAMP PMO

Note: The automated nature of Verizon's environment provides easier validation of the system



SD WAN circuit implementation

1

SD WAN-relevant circuit identification and mapping

In advance of the kickoff call, the full set of agency network connections and circuits would need to be identified, mapped and prioritized for the rollout to SD WAN.

This would include the following circuit migration activities:

- priority order
- circuit addresses
- bandwidth needs
- equipment requirements
- access needs (location, power, etc.)
- testing
- single pain of glass implementation

2

SD WAN testing, implementation and confirmation of operability

During the assessment process, extensive testing and work is required to ensure the SD WAN service is operating correctly.

- As the circuit inventory and other applications are documented and connected into the SD WAN application, Verizon and the agency will test to ensure the network is functioning properly.
- Overall circuit and SD WAN implementation complete and Verizon provides a confirmation to the agency of full system operability.

What is reviewed during the Security Assessment Report development?

The goal of the Security Assessment Report (SAR) is to independently evaluate (through the 3PAO) Verizon's security posture and parameters with respect to the guidelines outlined by the FedRAMP PMO.

The assessment will perform penetration testing, vulnerability scanning and manual testing of infrastructure, servers, storage, networking, virtualization software, services and management tools that support the computing requirements of Verizon's cloud computing model.

410 control points are evaluated during the assessment by the 3PAO.

Verizon's network platform is digital first, cutting edge which should assist in speeding up the implementation and approvals by FedRAMP.

Below are examples of the questions Verizon must fully answer during the assessment.

Documentation

- Are all documents in FedRAMP templates?
- Are all document artifacts complete?
- Are all ancillary SAR documents included with the SAR?

System Risks

- Are unique risks individually identified and labelled?
- Are risks described to a level of detail that could be understood by the ~~JAB~~ Agency Authorizing Official (AO)?
- Are HIGH findings identified and provided along with comments?
- Are downgraded risks listed, described, and include a description of the mitigating factor(s)?

Consistency

- Are the inventory lists in the SAR consistent with the lists provided in the SSP?
- Are the Assessment Results described in consistent with the Risk Exposure Table (SAR Section 4 and Appendix A)?
- Are document / system versions consistently stated within the SAR?

An example of a SAR [can be found here](#).

Note: 410 controls are required to be assessed by Verizon's system for FedRAMP High level certification. This is a more stringent evaluation than the assessment to obtain FedRAMP High Ready state.



Benefits of SD WAN for your agency

Verizon Managed Services can support your SD WAN and help your agency move forward confidently with your implementation. Some of the ways a Verizon-managed SD WAN solution can help are listed to the right.



Move from a traditional, IP address to an end-to-end, application-aware approach

Standardized SD WAN operational practice helps simplify consumption and speed transition.



Multiple access-service types and providers.

Verizon can bond multiple services into a single service with a unified view into performance reporting, change management and troubleshooting.



Update application routing rules as new users, applications and changing usage patterns impact WAN performance.

Tested change-management processes help your agency avoid unnecessary downtime from configuration errors.



Obtain accurate application inventory and applying reporting metrics to improve routing and utilization.

Verizon's reporting platforms and processes observe, analyze and recommend changes based on application behavior.



Integrate new reporting and change management platforms for application visibility.

Easily turn on and scale as a service platform, to support your agency's growing implementation with project management oversight for delivery.



Cost of hiring, training, building and maintaining application-centric routing and management systems, people and monitoring platforms.

Verizon provides geo-diversified network operations centers, trained personnel and scaled, carrier integrated management platforms with options for both shared and dedicated engineering resources.

Glossary of terms:

Below are some definitions that may come up in the ATO sponsorship process.

- **3PAO:** 3rd party assessment organization
- **ATO:** Authority to Operate
- **JAB:** Joint Authorization Board
- **POA&M:** The Plan of Action and Milestones (POA&M) documents Verizon's plan and timeline for remediating findings that remained at the conclusion of the security assessment.
- **RAR:** Readiness Assessment Report, which documents the service offering's system information, compliance with federal mandates, and ability to meet FedRAMP security requirements. This is what is needed to achieve FedRAMP Ready status.
- **SAR:** Security Assessment Report (SAR) independently evaluates Verizon's security parameters with respect to the guidelines outlined by the FedRAMP PMO.
- **SSP:** The System Security Plan (SSP) represents Verizon's overall security protocols regarding SD WAN.

What are the different stages of FedRAMP?

FedRAMP Ready: A designation provided to CSOs, which indicates that a 3PAO attests to a CSO's security capabilities, and that a FedRAMP Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by FedRAMP. FedRAMP Ready indicates a CSO has a high likelihood of successfully completing an initial FedRAMP authorization.

FedRAMP In Process: A designation provided to CSOs that are actively working toward a FedRAMP authorization. For updates, federal agencies can either contact the cloud provider via the email address provided on the CSO's FedRAMP Marketplace page, or reach out directly to FedRAMP via intake@fedramp.gov.

FedRAMP Authorized: A designation provided to CSOs that have successfully completed the FedRAMP authorization process. FedRAMP Authorized CSOs are available for government-wide reuse.

Contact us today

For more information on how you can partner with Verizon to ensure our ATO's are in optimal alignment with your agency's mission needs, contact us at:

govinfo@verizon.com

verizongov.com

